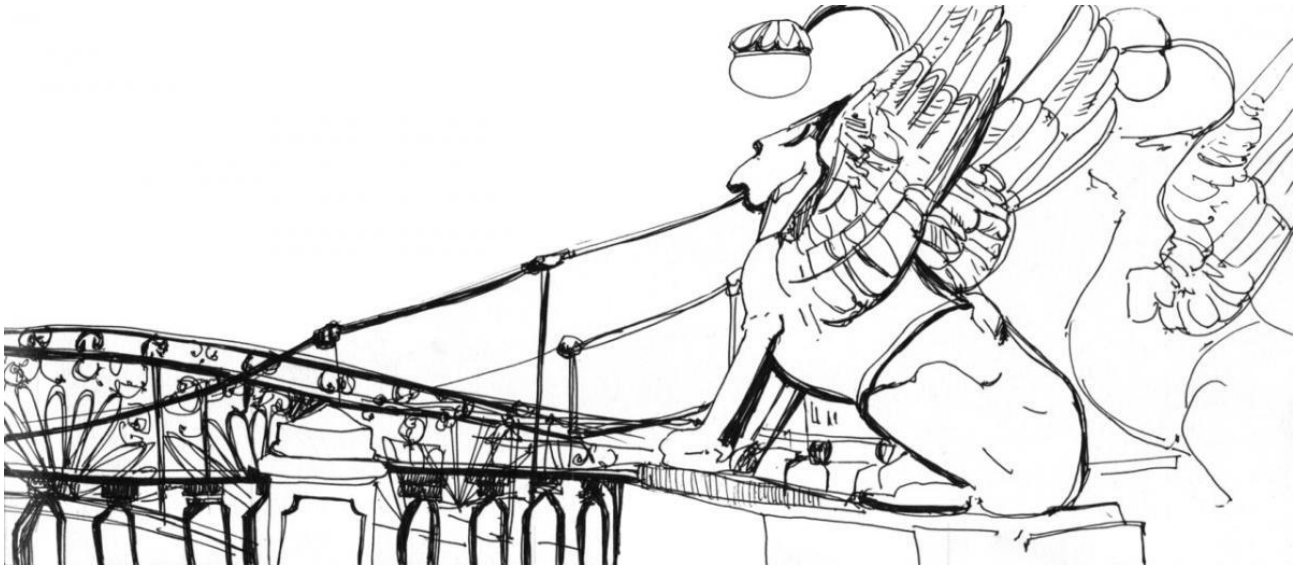
ГУМАНИТАРНЫЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ИНСТИТУТ «НАЦРАЗВИТИЕ»

№1(3) Январь 2022

НАЦБЕЗОПАСНОСТЬ

НАУЧНЫЙ ЖУРНАЛ

ПЕРИОДИЧЕСКОЕ ПЕЧАТНОЕ ИЗДАНИЕ



ГНИИ «НАЦРАЗВИТИЕ»
САНКТ-ПЕТЕРБУРГ
2022

«НАЦБЕЗОПАСНОСТЬ»
НАУЧНЫЙ ЖУРНАЛ
Выходит 1 раз в 2 месяца
№1(3) Январь 2022

ISSN: 2782-3083
DOI 10.37539/2782-3083.2022.3.1.001

Н35 Нацбезопасность: научный журнал. – № 1(3). СПб., Изд. ГНИИ «Нацразвитие», Январь 2022. – 40 с.

Общероссийский печатный научный журнал, публикующий результаты фундаментальных, поисковых и прикладных исследований, выполненных по различным наукам с позиций безопасности.
Целевая аудитория издания – сообщество исследователей и практиков научных институтов, лабораторий, учреждений образования, органов управления, соискатели ученой степени, студенчество.

Журнал
издается с 2021 года

Учредитель:
ЧНОУДПО Гуманитарный национальный исследовательский институт «НАЦРАЗВИТИЕ»

Адрес редакции, издателя и типографии:
197348, г. Санкт-Петербург,
Коломяжский пр-т, д. 18, лит. А
тел. (812) 905-29-09
http://natsrazvitie.ru
info@natsrazvitie.ru

Полнотекстовая версия журнала
размещается на сайте:
http://natsrazvitie.ru/nauchnyy_zhurnal_nacbezopasnost/

Выходные данные:
ГНИИ «НАЦРАЗВИТИЕ»
САНКТ-ПЕТЕРБУРГ
2022

Выпускные данные:
Свидетельство о регистрации средства массовой информации *ПИ № ФС77-80721 от 29 марта 2021 г.* выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзором)

Подписано в печать с оригинал-макета 14.01.2022. Формат 60х84 1/8. Печать цифровая. Гарнитура Times New Roman. Усл. печ. л. 2,9. Тираж 100 экз. Заказ № 20217. Отпечатано в типографии ЧНОУДПО ГНИИ «Нацразвитие»

ВСЕРОССИЙСКИЙ ПЕЧАТНЫЙ НАУЧНЫЙ ЖУРНАЛ «НАЦБЕЗОПАСНОСТЬ»

НБ РАЗДЕЛ.
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004
DOI 10.37539/2782-3083.2022.3.1.002

Зейкан Михаил Викторович,
КФ МГТУ им. Н.Э. Баумана, г. Калуга
Zeykan Mihail Viktorovich, KB of BMSTU, Kaluga

Вершинин Евгений Владимирович,
к.ф.-м.н., доцент, КФ МГТУ им. Н.Э. Баумана, г. Калуга
Vershinin Evgeniy Vladimirovich, KB of BMSTU, Kaluga

Фёдоров Виктор Олегович, к.т.н., доцент,
КФ МГТУ им. Н.Э. Баумана, г. Калуга
Fedorov Victor Olegovich, KB of BMSTU, Kaluga

ПРОБЛЕМА ЗАЩИТЫ ДАННЫХ ПРИ ПРОЕКТИРОВАНИИ ВЕБ-ПРИЛОЖЕНИЯ
THE PROBLEM OF DATA PROTECTION WHEN DESIGNING A WEB APPLICATION

Аннотация: в статье приведены базовые меры повышения защиты веб-приложений. Расписан менеджмент уязвимостей. Указаны эффективные способы защиты информации в базах данных.

Abstract: the article provides basic measures to improve the protection of web applications. Vulnerability management is described. Effective ways of protecting information in databases are indicated.

Ключевые слова: защита данных, менеджмент уязвимостей.

Keywords: data protection, vulnerability management.

Организации пытаются как можно чаще применять веб-технологии как основу для оптимизации бизнес-процессов с помощью разных систем для работы с данными. Это имеет свои преимущества, но и добавляет в информационную систему новые угрозы. Рассмотрим защиту данных в веб-приложениях, основанных на трехуровневой архитектуре, когда пользователь через браузер обращается не напрямую к серверу баз данных, а к серверу приложений, от которого идет запрос данных к базе данных.

Введение

Трехуровневая архитектура имеет огромное количество составляющих: рабочие места сотрудников, серверы приложений, СУБД, базы данных, каналы связи. Все компоненты представляют собой потенциальный источник утечки информации:

- перехват трафика до и после сервера веб-приложения;
- получение информации через уязвимости веб-приложения;
- хищение информации сотрудниками, не имеющими доступ;
- выгрузка информации напрямую из базы данных.

Однако внедрение всех возможных средств защиты часто не оправдано. Для построения эффективной и достаточной системы защиты необходимо:

- провести полный аудит защищаемого приложения;
- установить ценность обрабатываемой информации;
- составить уровни доступа пользователей к данным;
- определить слабые места и самые вероятные точки утечки информации.

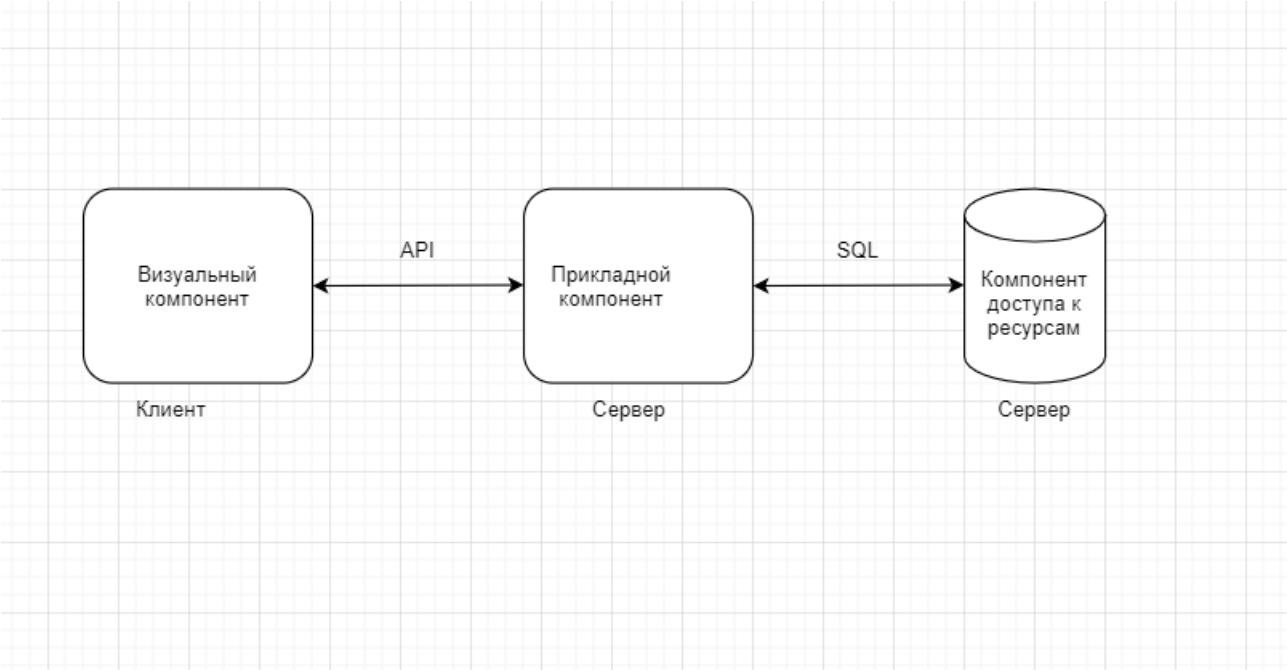


Рисунок 1 – Трехуровневая защита

Базовые меры повышения уровня защиты веб-приложений

Первый шаг к обеспечению защищенности – правильная настройка всех модулей системы, обновление всего используемого программного обеспечения до актуальных версий, отключение всех неиспользуемых служб, смена всех паролей по умолчанию, отключение неиспользуемых учетных записей, в том числе системных. Важно также обеспечить шифрование данных всех сетевых соединений внутри системы. В случае если это позволяет веб-приложение, необходимо настроить разграничение прав доступа пользователей к данным и настройкам системы, ограничив их минимально необходимыми.

В простых случаях уже только перечисленные базовые меры позволят снизить риски до допустимого уровня. Если базовых мер окажется недостаточно, необходимо обратить внимание на разнообразные специализированные средства защиты информации[1].

Аутентификация пользователей как слабое звено веб-приложений

Одно из наиболее известных слабых мест – это аутентификация пользователей веб-приложения. Система при регистрации пользователя не проводит проверку на сложность пароля, или пароль не имеет срока действия, или при аутентификации пароль от браузера передается к серверу в URL запросе.

Для устранения подобных проблем существуют решения для усиления аутентификации в веб-приложении, реализованные как в виде встраиваемых модулей, так и в виде отдельных серверов аутентификации.

Встроенная в приложение аутентификация позволяет не использовать внешние средства аутентификации, однако это не исключает возможные ошибки в самом веб-приложении, позволяющие обойти систему аутентификации. Решить эту проблему можно путем внедрения процесса менеджмента уязвимостей.

Менеджмент уязвимостей

Если в компании используются приложения, разработанные на заказ сторонним подрядчиком, и исходный код приложений недоступен, сотрудникам информационной безопасности при приемке программного обеспечения имеет смысл использовать сканер уязвимостей, который работает с веб-приложением по принципу «черного ящика». При нахождении критических уязвимостей приложение возвращается на доработку разработчику.

В случае, когда веб-приложение является внутренней разработкой компании, рекомендуется выстраивать процесс безопасной разработки программного обеспечения с использованием анализаторов исходного кода, проверяя весь разрабатываемый код на отсутствие

ошибок, приводящих к уязвимостям. Такой подход позволяет исправить ошибки в приложении на раннем этапе и избежать лишних затрат. Большинство анализаторов кода позволяет проводить как статический анализ кода без его выполнения, так и динамический, проверяя уже установленное и запущенное приложение. В последнем случае требуется указание точек входа и большое количество входных данных.

Сочетание перечисленных методов позволяет выявлять уязвимости до внедрения приложений в компании. В то же время реализация в компании процессов верификации приложений может потребовать значительных материальных и временных затрат. Иногда просто нет возможности оперативно вносить изменения в уже работающее приложение. Если ценность данных не позволяет закрыть глаза на возможные уязвимости, имеет смысл рассмотреть возможность использования специализированных средств защиты веб-приложений – Web Application Firewall. Существуют как коммерческие, так и свободно распространяемые системы.

Принцип работы специализированной защиты WAF

Принцип работы WAF: HTTP-трафик от пользователей до веб-приложения проходит сначала через WAF либо, в зависимости от задач и возможностей, на WAF направляется копия трафика. Далее трафик подвергается декодированию и проверке на наличие атак. Если WAF установлен «в разрыв» (прокси, мост), атаки могут быть заблокированы. В пассивном режиме работы (копия трафика) возможны только мониторинг и оповещение об атаках. Для обнаружения атак могут использоваться такие методы, как:

- сигнатурный анализ;
- репутационные списки;
- автоматическое обучение;
- поведенческий анализ;
- вручную настраиваемые правила.

Кроме этого, WAF может иметь модули для динамического анализа уязвимостей защищаемых приложений, виртуального обновления найденных багов, управления аутентификацией пользователей, взаимодействия с другими системами защиты. Все это позволяет снизить количество актуальных для веб-приложения угроз.

Эффективные способы защиты информации в базах данных

Опасность для информации в веб-приложении представляют и внутренние нарушители – сотрудники, которые имеют доступ к данным для выполнения служебных обязанностей, администраторы с прямым доступом к серверу баз данных (в обход веб-приложения или локально). В этом случае для обеспечения безопасности веб-приложений возможно использовать решения, реализующие разный подход к мониторингу и контролю обращений к базам данных[2].

Системы защиты информации в базах данных можно разделить на три типа:

1. Системы, использующие принцип работы, схожий с WAF, – перехват трафика, но идущего не от пользователя до сервера приложений, а от сервера приложений к серверам баз данных. Производится декодирование протоколов баз данных с последующим анализом, используя правила, настроенные сотрудником информационной безопасности. Возможна работа в активном (блокирующем) режиме, для этого система устанавливается «в разрыв» (прокси, мост), а также в пассивном режиме мониторинга, для этого достаточно подать копию трафика. Для контроля локальных и прямых сетевых подключений к базам данных используются агенты, устанавливаемые непосредственно на серверы баз данных. При использовании таких систем для защиты данных в веб-приложениях с трехзвенной архитектурой может возникнуть сложность с определением пользователя, сделавшего запрос к базе данных: в трафике, идущем от сервера приложений, все обращения производятся от служебной учетной записи. Для персонификации сотрудника предусмотрена интеграция с WAF, который анализирует трафик до сервера приложений, либо подача копии этого трафика непосредственно на систему защиты баз данных. Также в системах рассматриваемого типа могут быть реализованы возможности, косвенно повышающие защищенность:

- сканирование на уязвимости баз данных;
- обнаружение баз данных;
- маскирование критичной информации, например, номеров кредитных карт;
- создание матрицы разграничения прав доступа;
- мониторинг изменений, позволяющий вовремя отследить несанкционированное повышение прав пользователя.

2. В случаях, когда возможность анализа копии трафика отсутствует или необходимо применить маскирование и блокировки, но установить систему защиты «в разрыв» невозможно, используются решения, основанные на других принципах перехвата обращений пользователей к базам данных. Такие решения используют в качестве точки съема агент, устанавливаемый на защищаемый сервер приложения и взаимодействующий с драйверами, через которые веб-приложение передает запросы пользователей к базам данных. Т.к. агент находится на сервере веб-приложения, он обрабатывает и запросы клиентов приложению и запросы приложения к базам данных, персонифицируя запросы. Создавая правила обработки запросов, можно маскировать «на лету» любые поля в ответах от базы данных, блокировать запросы сторонних лиц, полностью управлять бизнес-процессом работы пользователя с приложением[3].

3. Системы защиты информации от утечек, основанные на использовании криптографии и позволяющие выборочно шифровать информацию, хранящуюся в таблицах баз данных. Доступ к информации предоставляется только авторизованным пользователям, с ведением детальных протоколов их действий. Для повышения защищенности информации такие системы могут дополнительно реализовывать механизмы строгой двухэтапной аутентификации.

Использование перечисленных средств позволит существенно снизить риск утечки данных из веб-приложения, а при инцидентах поможет отыскать необходимую для расследования информацию.

Последний этап защиты – правильное хранение резервных копий баз данных: если средства шифрования при работе с базой данных не используются, необходимо шифровать ее копии[4].

Выводы

Выбор средств защиты веб-приложений является комплексной задачей и не ограничивается использованием исключительно WAF-решений. Необходимо взвешенно оценивать угрозы, использовать данные аудита защищенности веб-приложений, а также учитывать особенности инфраструктуры и процессов обработки данных. И важным для проектирования и внедрения рассматриваемого класса решений является также привлечение профессиональных команд исполнителей.

Список литературы:

1. Горев А.В. Интеллектуальный анализ защиты данных // Безопасность информационного пространства. Сборник трудов XIX Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых. Екатеринбург, 2021 С. 10-14.

2. Оралбаев Е.А. Обнаружения проблем в безопасности веб-приложений // Актуальные вопросы современной науки и образования. Монография. Пенза, 2021 С. 190-200.

3. Савченко Е.В., Ниссенбаум О.В. Ботнет-атаки на устройства интернета вещей // Математическое и информационное моделирование. Сборник научных трудов, электронный ресурс. Тюмень, 2018 С. 347-356.

4. Тавасиев Д.А., Команов П.А., Ревазов Х.Ю., Семиков В.С. Анализ методов выявления уязвимостей во встроенном программном обеспечении // Международный научно-исследовательский журнал. 2020 № 1-1 (91). С. 34-37.

НБ РАЗДЕЛ. КИБЕРБЕЗОПАСНОСТЬ И КИБЕРПРЕСТУПНОСТЬ

УДК 004

Лобова Анастасия Игоревна,
КФ МГТУ им. Н.Э. Баумана, г. Калуга
Lobova Anastasia Igorevna, KB of BMSTU, Kaluga

Вершинин Евгений Владимирович,
к.ф.-м.н., доцент, КФ МГТУ им. Н.Э. Баумана, г. Калуга
Vershinin Evgeniy Vladimirovich, KB of BMSTU, Kaluga

Фёдоров Виктор Олегович, к.т.н., доцент,
КФ МГТУ им. Н.Э. Баумана, г. Калуга
Fedorov Victor Olegovich, KB of BMSTU, Kaluga

ОБЗОР DDOS-АТАК НА IOT УСТРОЙСТВА
OVERVIEW OF DDOS ATTACKS ON IOT DEVICES

Аннотация: распределенные атаки типа «отказ в обслуживании» становятся одной из самых глобальных угроз в сети Интернет. Растущее число устройств интернета вещей увеличивает множество способов проведения DDoS атак. В данной статье проведен обзор DDoS-атак на устройства интернета вещей и приведены основные рекомендации по защите ИТ-инфраструктур с устройствами IoT.

Abstract: distributed denial of service attacks are becoming one of the most global threats on the Internet. The growing number of IoT devices increases the variety of ways DDoS attacks can be carried out. This article provides an overview of DDoS attacks on IoT devices and provides basic recommendations for protecting IT infrastructures with IoT devices.

Ключевые слова: DDoS, IoT, ботнет, отказ в обслуживании, Mirai.

Keywords: DDoS, IoT, botnet, denial of service, Mirai.

Введение

DDoS-атаки (Distributed Denial of Service – распределённые атаки класса «отказ в обслуживании») – это атаки на вычислительные системы (сетевые ресурсы или каналы связи), имеющие целью сделать их недоступными для легитимных пользователей. DDoS-атаки заключаются в одновременной отправке в сторону определенного ресурса большого количества запросов с одного или многих компьютеров, расположенных в сети Интернет. Если тысячи, десятки тысяч или миллионы компьютеров одновременно начнут посылать запросы в адрес определенного сервера (или сетевого сервиса), то либо не выдержит сервер, либо не хватит полосы пропускания канала связи к этому серверу. В обоих случаях, пользователи сети Интернет не смогут получить доступ к атакуемому серверу, или даже ко всем серверам и другим ресурсам, подключенным через заблокированный канал связи [8].

Иными словами, DDoS-атака – атака, направленная на замедление работы или выведение из строя серверов, сетевой инфраструктуры, а также бомбардировка трафика приложений из нескольких ресурсов. В результате DDoS-атак сайты и приложения становятся заторможенными либо вообще перестают работать. В настоящее время более 30% случаев простоя приложений и серверов вызваны DDoS-атаками [1].

В глобальном масштабе ежедневно регистрируется две тысячи DDoS-атак. Средняя атака DDoS обходится крупной компании в 250 долл. в час [2].

Ботнеты как самый популярный и опасный способ проведения DDoS-атак

Наиболее популярным и опасным способом запуска DDoS-атак является использование ботнетов (BotNets).

Ботнет – это сеть девайсов, инфицированных вредоносным ПО, дающим злоумышленнику доступ к удаленному контролю над ними, к рассылке спама и вирусов, а особенно служащих местом размещения ПО, осуществляющим DDoS-атаки без ведома владельца зараженного гаджета.

Однако, в частности, говоря об «интернете вещей», ботнет – это сеть инфицированных вредоносным ПО IoT устройств [1].

Боты распространяются в сети Интернет различными способами, как правило – путем атак на компьютеры, имеющие уязвимые сервисы, и установки на них программных закладок, либо путем обмана пользователей и принуждения их к установке ботов под видом предоставления других услуг или программного обеспечения, выполняющего вполне безобидную или даже полезную функцию. Способов распространения ботов много, новые способы изобретаются регулярно.

Если ботнет достаточно большой – десятки или сотни тысяч компьютеров – то одновременная отправка со всех этих компьютеров даже вполне легитимных запросов в сторону определённого сетевого сервиса (например, web-сервиса на конкретном сайте) приведет к исчерпанию ресурсов либо самого сервиса или сервера, либо к исчерпанию возможностей канала связи. В любом случае, сервис будет недоступен пользователям, и владелец сервиса понесет прямые, косвенные и репутационные убытки. А если каждый из компьютеров отправляет не один запрос, а десятки, сотни или тысячи запросов в секунду, то ударная сила атаки увеличивается многократно, что позволяет вывести из строя даже самые производительные ресурсы или каналы связи [8].

DDoS-атаки на IoT устройства

Случаи бурного роста числа и тяжести DDoS атак, зарегистрированные в 2016-2017 годах, вызваны широким внедрением технологии Internet of Things (IoT) [1].

IOT – это развивающаяся технология, которая объединяет обычные устройства с Интернетом. После подключения к сети IoTD (устройства интернета вещей) могут обмениваться данными друг с другом, веб-службами и приложениями. Интернет вещей используется для обеспечения человека такими удобствами, таких как автоматическое или удаленное управление умными домами, эффективная инфраструктура с низким уровнем отходов, а также сбор и анализ биометрических данных в реальном времени с помощью носимых технологий.

Хотя устройства Интернета вещей (IoTD) приносят пользу во многих аспектах жизни, эти устройства также создают риски безопасности в виде уязвимостей, которые дают хакерам миллиарды новых многообещающих целей. Например, ботнеты использовали недостатки безопасности, характерные для IoTD, для получения несанкционированного контроля над сотнями тысяч хостов, которые затем использовали для проведения массовых разрушительных распределенных атак типа «отказ в обслуживании» [3].

На данный момент концепция IoT опирается на две технологии:

1) Радиочастотная идентификация – метод распознавания объектов, при котором благодаря использованию радиосигналов происходит записывание и считывание имеющихся данных;

2) Беспроводные сенсорные сети – наличие множества датчиков и исполнительных устройств, объединенных с помощью радиосигнала, область покрытия которого находится в диапазоне от нескольких метров до пары километров.

Архитектура IoT предполагает наличие следующих уровней: сеть датчиков, шлюз, управление, приложение. Большинство сервисов IoT основано на обработке информации от множества узлов, что принципиально отличается от архитектур классических сетей. Поэтому необходимы специальные протоколы для обеспечения взаимодействия устройств друг с другом и верхними уровнями [4].

Одной из основных причин уязвимости информационных систем в сети Интернет, в том числе IoT, являются слабости сетевого протокола IP стека протоколов TCP/IP, который служит основой сетевых коммуникаций.

Ботнеты для IoT отличаются от аналогов на базе Windows тем, что они построены из взломанных IoT-устройств и могут распространяться на огромное количество устройств, используя обширную сеть IoT. Более того, в отличие от обычных ботнетов, которые, в основном, используются для рассылки спама, ботнеты IoT могут нанести гораздо больший ущерб, воздействуя на доступную для устройств IoT физическую среду.

Например, атака ботнетов IoT на светофоры может создать хаос в городе и разрушать интеллектуальную городскую инфраструктуру. Аналогичным образом хакеры способны увеличить температуру в умных домах и искусственно повысить спрос на нефть или газ.

В отличие от персональных компьютеров и серверов, которые защищены фильтрующими функциями файерволов и детекторами вредоносных программ, IoT-устройства становятся для ботнетов привлекательными целями, поскольку они обычно не используют такие расширенные функции безопасности.

Угроза для кибербезопасности, связанная с распространением ботсетей IoT, была предсказана в 2016 году, но специалисты по безопасности в Интернете не уделили достаточно внимания этой проблеме. В то время эта угроза представлялась довольно ограниченной. Однако вскоре появился набор инструментов, позволяющих ботнетам пользоваться уязвимостью в незащищенных устройствах IoT. Атака Mirai в октябре 2016 года стала ключевым поворотным моментом в развитии IoT.

Злоумышленникам не так интересны IoT девайсы в качестве «жертвы». Цель хакеров – захватить устройство, чтобы добавить его к ботнету, который и используется для DDoS-атак.

Безопасность «интернета вещей» в целом недооценивается и даже игнорируется не только обычными пользователями, но и целыми компаниями. Именно из-за уязвимости IoT устройств и их растущего количества данная область интернета интересна хакерам [1].

Вместе с ежегодным ростом количества IoT устройств, растет потенциальное количество уязвимостей во встроенном программном обеспечении этих устройств. От того насколько быстро будет обнаружена уязвимость, зависит скорость выпуска патча, закрывающего эту уязвимость, следовательно существует потребность в повышении эффективности процесса выявлении уязвимостей во встроенном программном обеспечении устройств интернета вещей [5].

Интернет вещей присутствует в различных устройствах: в бытовой технике, смартфонах, умной одежде, носимых устройствах (браслеты, очки виртуальной реальности и т.д.), смарт-телевизорах, игровых консолях, транспортных системах, зданиях (камеры видеонаблюдения), кондиционирование воздуха, контроль доступа и т. д.), общественные инфраструктуры (мосты, шоссе, парки и т. д.), общественные услуги, промышленные компоненты (например, системы SCADA), системы транспортировки и т. д.

По мере увеличения сбора и анализа информации с различных устройств, не только промышленный сектор и сектор услуг, но и вся технологическая инфраструктура, на которой основано общество, подвергается опасности, что увеличивает риски безопасности, где объем данных растет со все возрастающей скоростью, превышающей несколько эксабайтов. Несанкционированный доступ организованной преступности к системам прогнозирования в промышленной, военной, финансовой, медицинской и иной инфраструктуре может быть критичен и практически непоправим [6].

Не каждая компьютерная система в доме содержит сканер вирусов: в современном доме вы легко найдёте больше десятка устройств на базе Linux и процессоров ARM или MIPS, – телевизоры, работающие под управлением смарт-систем, сетевые устройства, такие как точки доступа и адаптеры Powerline, интернет-радио и Raspberry Pi.

Отсутствие программного обеспечения безопасности и, в частности, отсутствие мер безопасности, интегрированных в Linux, повышают привлекательность для хакеров. Поскольку вредоносное ПО обычно запускается и удаляется, то есть исчезает после перезапуска, ни анализ образа операционной системы, ни проверка существующих файлов не помогают.

Mirai как один из самых опасных ботнетов, нацеленных на IoT

Mirai – это вредоносная программа, которая заражает интеллектуальные устройства, работающие на процессорах ARC, превращая их в сеть удаленно управляемых ботов или «зомби». Эта сеть ботов часто используется для запуска DDoS-атак.

Mirai сканирует Интернет на предмет устройств IoT, работающих на процессоре ARC. Этот процессор работает под управлением урезанной версии операционной системы Linux. Если комбинация имени пользователя и пароля по умолчанию не изменена, Mirai сможет войти в устройство и заразить его.

Mirai со временем мутирует. Злоумышленники, пользуясь его исходным кодом, оставшимся в сети, разработали и продолжают разрабатывать другие ботнеты, такие как Okiru, Satori, Masuta и PureMasuta.

Мутации Mirai начали появляться буквально ежедневно, и то, что у них сохранялась способность размножаться и наносить ущерб с помощью тех же методов, что и у оригинала, указывает на хроническое пренебрежение производителей устройств Интернета вещей простейшими методами защиты. Как ни странно, при этом ботнеты, образованные из таких устройств, исследовались слабо, несмотря на опасность того, что все более сложные атаки на их базе потенциально способны подорвать всю инфраструктуру Интернета [7].

Особенность сканирования устройств ботнетом Mirai заключается в словаре логинов и паролей, которые бот использует при попытках подключения к устройству. Так, например, автор оригинального Mirai включил в процесс сканирования относительно небольшой список логинов и паролей для подключения к различным устройствам. Однако в настоящее время зафиксировано значительное расширение этого списка за счет логинов и паролей «по умолчанию» от различных IoT-устройств, что говорит о появлении модификаций данного бота.

Существует также недавно обнаруженный и мощный ботнет, получивший различные прозвища IoTrooper и Reaper, который может взламывать устройства Интернета вещей гораздо быстрее, чем Mirai. Reaper способен нацеливаться на большее количество производителей устройств и имеет гораздо больший контроль над своими ботами [7].

Традиционные стратегии обнаружения DDoS-атак

1) Обнаружение на основе подписи. Существует два распространенных подхода к обнаружению продолжающихся DDoS-атак: на основе сигнатур и на основе аномалий. Обнаружение на основе сигнатур обычно пытается сопоставить доступные данные с известными шаблонами атак. Пример этого можно увидеть в Captcha, которая представляет собой соединение систем с задачей, которую легко решить для человека, но которая превосходит возможности современных компьютерных программ. Этот подход имеет преимущество простоты; при обнаружении новой атаки можно идентифицировать уникальные характеристики ее активности и добавить их в базу данных сигнатур.

Ботнет Mirai, например, представляет отличительные сигнатуры сетевого трафика на этапах сканирования и заражения, что делает его сильным кандидатом для обнаружения на основе сигнатур.

2) Обнаружение аномалий. Обнаружение на основе аномалий идентифицирует атаки, основанные на отклонении от нормы. Типичная реализация этой стратегии заключается в том, что механизм обнаружения изучает нормальное состояние системы, наблюдая за ним в течение длительного периода времени. Когда он обнаруживает необычную активность, он поднимает тревогу. Распространенной стратегией для обнаружения аномалий является статистическое моделирование работы системы, создание математической основы для определения того, что является нормальным, а что нет. Поскольку этот метод не использует узкую сигнатуру для обнаружения атак, он может идентифицировать атаки нулевого дня, замечая странную активность в системе, которую он отслеживает.

К сожалению, обнаружение аномалий тоже не лишено недостатков. Хотя система может столкнуться с очень необычным состоянием, это не обязательно означает, что она находится под атакой.

Системы обнаружения аномалий по своей природе имеют тенденцию к чрезмерному усердию при обозначении активности как атаки, что приводит к тому, что они характеризуются высоким уровнем ложных тревог [3].

Несмотря на то, что полностью искоренить угрозу бот-сетей невозможно, все еще есть способы ограничить воздействие и масштабы этих атак, приняв превентивные меры. Один из них – размещение устройств Интернета вещей в сегментированной сети, защищенной от внешнего трафика. Также крайне важно начать мониторинг систем и инвестировать в разработку процессов обнаружения вторжений, которые будут иметь большое значение для предупреждения пользователя о том, что система взломана.

Помимо сегментации и тестирования сети, не стоит забывать о фундаментальных мерах безопасности, таких как своевременное обновление прошивки и программного обеспечения, а также возможность контролировать, кто может получить доступ к определенному устройству [9].

Основные рекомендации по защите ИТ-инфраструктур в эпоху IoT

Защита от DDoS и других типов кибератак начинается с понимания сложности современных угроз безопасности. Интернет Вещей представил новые проблемы безопасности для обоих предприятий, которые делают связанные гаджеты частью своих ИТ-инфраструктур и компаний, которые управляют всеми видами веб-решений, включая корпоративные веб-сайты, CRM-системы и настраиваемые социальные сетевые решения.

Следуя этим общим, но эффективным, советам, вы сможете значительно снизить риски безопасности, связанные с IoT, и обеспечить безопасность ИТ-инфраструктуры:

• Никогда не забывайте переустанавливать пароли по умолчанию и обновлять прошивку. Использование паролей устройств IoT по умолчанию является основной причиной, по которой произошла атака Mirai. 47% ИТ-отделов добавили новые подключенные гаджеты в свои корпоративные сети, не изменяя пароли, установленные производителями устройств. Если вы перейдете в интерфейс управления и обнаружите, что пароли по умолчанию не могут быть изменены, не стесняйтесь удалять гаджеты из корпоративной сети, а лучше вообще не приобретать такие устройства. То же самое касается обновлений прошивки, которые должны выполняться автоматически или, по крайней мере, требуют небольшого надзора со стороны ИТ-команды.

• Не выставляйте устройства напрямую в Интернет – решения IoT, которые обрабатывают большие объемы данных и, следовательно, требуют высокоскоростной полосы пропускания – например, камеры видеонаблюдения, которые составляют большую часть армии бота Mirai, – всегда должны быть защищены брандмауэром. Кроме того, вы можете использовать сторонний порт и решения сканирования трафика, такие как BullGuard, чтобы определить, публично ли открыт IP-адрес и обнаружить устройства с открытыми портами.

• Работа с надежными поставщиками IoT. Наиболее известные уязвимости устройства IoT, в том числе неправильное использование механизмов аутентификации и авторизации, отсутствие шифрования транспортного уровня и проблемы с исправлением прошивки, обусловлены плохими решениями, принятыми в ходе разработки программного обеспечения IoT. Если вы рассматриваете возможность внедрения стороннего или настраиваемого подключенного решения на рабочем месте, обязательно обратитесь к компаниям с проверенной репутацией в разработке решений IoT.

• Укрепление безопасностью веб-приложений. Плохая новость об атаках, вызванных IoT-атак, заключается в том, что любая компания или физическое лицо, независимо от того, используют ли они решения IoT для деловых целей или нет, могут легко попасть под огонь. Существует несколько способов защиты ваших веб-приложений от бот-сетей IoT. Во-первых, вы можете реализовать решение VPN для маскировки своего веб-трафика. Во-вторых, используйте безопасные готовые плагины CMS и другие программные компоненты с открытым исходным кодом без документированных уязвимостей безопасности. И, наконец, вы никогда не должны идти на компромисс по обеспечению качества [10].

• Отключайте функции, которые не будут использоваться.

• Отслеживайте журнал работы. Например, что делал регулятор тепла, пока вас не было дома.

• Используйте специально разработанные для умного дома антивирусные программы, которые защитят ваши устройства от атак ботнетов.

• Если вы используете управление через голосовые команды, то пробуйте иногда менять фразы для их активации.

• Отключите протокол UPnP (Universal Plug & Play). UPnP находит схожие устройства и подключается к ним. Однако такой протокол вредоносное ПО также может взламывать ввиду наличия уязвимостей. То есть если предмет умного дома соединен с другим предметами, то они также будут заражены.

Выводы

С распространением технологии Интернета вещей компьютерные сети быстро увеличиваются в размерах. Хотя устройства Интернета вещей приносят пользу во многих аспектах жизни, они также создают риски безопасности в виде уязвимостей, которые дают хакерам миллиарды новых целей. Именно поэтому необходима защита устройств Интернета вещей не только со стороны разработчиков программного обеспечения, но и, главным образом, со стороны пользователей. Следуя общим, но эффективным правилам, пользователи могут значительно снизить риски безопасности, связанные с IoT, и обеспечить безопасность как отдельных устройств, так и всей ИТ-инфраструктуры.

Список литературы:

1. Баженов А.С. Обзор DDoS атак на IoT устройства // Наука настоящего и будущего. 2019. Т. 1. С. 122-125.

2. Горев А.В. Интеллектуальный анализ DDoS-атак ботнета на IoT устройства при помощи Sap Analytics Cloud // Безопасность информационного пространства. Сборник трудов XIX Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых. Екатеринбург, 2021. С. 10-14.

3. Оралбаев Е.А. Обнаружения DDoS-атак ботнетов в сетях доступа IoT // Актуальные вопросы современной науки и образования. Монография. Пенза, 2021. С. 190-200.

4. Савченко Е.В., Ниссенбаум О.В. Ботнет-атаки на устройства интернета вещей // Математическое и информационное моделирование. сборник научных трудов, электронный ресурс. Тюмень, 2018. С. 347-356.

5. Тавасиев Д.А., Команов П.А., Ревазов Х.Ю., Семиков В.С. Анализ методов выявления уязвимостей во встроенном программном обеспечении IoT устройств // Международный научно-исследовательский журнал. 2020. № 1-1 (91). С. 34-37.

6. Díaz J. Internet of Things and Distributed Denial of Service as Risk Factors in Information Security: [Электронный ресурс]. URL: https://www.intechopen.com/chapters/73910. (Дата обращения: 25.10.2021).

7. What is the Mirai botnet?: [Электронный ресурс] // Cloudaflare. URL: https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/. (Дата обращения: 20.11.2021).

8. DDoS-атаки и как от них защищаться. Систематизация мирового и российского опыта: [Электронный ресурс] // Nag. URL: https://nag.ru/material/16862. (Дата обращения: 10.11.2021).

9. IoT Botnets and DDoS Attacks: Architecting Against Disaster: [Электронный ресурс] // IoT for all. URL: https://www.iotforall.com/iot-botnets-ddos-attack-architecture. (Дата обращения: 15.11.2021).

10. Взгляд внутрь инициированных IoT DDoS-атак и защита ИТ-инфраструктур: [Электронный ресурс] // SecurityLab. URL: https://www.securitylab.ru/blog/personal/bezmaly/344271.php. (Дата обращения: 11.11.2021).

НБ РАЗДЕЛ. ВОПРОСЫ ПРОМЫШЛЕННОЙ БЕЗОПАСНОСТИ

УДК 614.8.084

Фахретдинова Гульназ Ильдаровна, магистрант,
Уфимский государственный нефтяной технический университет, г. Уфа
Fakhretdinova Gulnaz Ildarovna, Ufa State Petroleum Technological University, Ufa

Идрисов Роберт Хабибович, доктор техн. наук, профессор,
Уфимский государственный нефтяной технический университет, г. Уфа
Idrisov Robert Habibovich, Ufa State Petroleum Technological University, Ufa

ОСОБЕННОСТИ АТТЕСТАЦИИ РАБОТНИКОВ ПО ПРОМЫШЛЕННОЙ БЕЗОПАСНОСТИ В ООО ИК «СИБИНТЕК»
FEATURES OF EMPLOYEE CERTIFICATION FOR INDUSTRIAL SAFETY IN LLC IK «SIBINTEK»

Аннотация: соблюдение современных требований промышленной безопасности является неотъемлемой частью любого производственного процесса. Предприятия добывающей отрасли можно отнести к опасным производственным объектам, чья промышленная безопасность регулируется разработанным комплексом действующих законодательных актов, нормативов, стандартов и иных действующих регламентов различного значения.

Abstract: compliance with modern industrial safety requirements is an integral part of any production process. Extractive industry enterprises can be classified as hazardous production facilities, whose industrial safety is regulated by a developed set of existing legislative acts, regulations, standards and other applicable regulations of various meanings.

Ключевые слова: промышленная безопасность, системы обучения, аттестации работников, предприятия добывающей отрасли, производственные объекты.

Keywords: industrial safety, training systems, certification of workers, extractive industry enterprises, production facilities.

Введение

Основной целью охраны труда является создание безопасных условий для работы на предприятии, а промышленная безопасность направлена на снижение риска аварий на потенциально опасных производственных объектах (ОПО). Так или иначе, эти две сферы пересекаются в области заботы о здоровье и жизни людей.

Опасные производственные объекты всегда связаны с риском для жизни сотрудников. Поэтому задача специалиста по промышленной безопасности – создать систему предотвращения аварий на предприятии. Но, несмотря на то что промбезопасность – более узкая и технически ориентированная область, в ней нельзя обойтись без отлаженных механизмов работы службы по охране труда [3].

Создание безопасных условий труда, сохранение жизни и здоровья работников, обеспечение наиболее надежной и бесперебойной работы действующих опасных производственных объектов, а также обеспечение полной пожарной безопасности и соответственно смежной безопасности дорожного движения должны являться одним из приоритетных направлений деятельности добывающей газа, газового конденсата и нефти компании [2].

Обучение по программам промбезопасности в 2021 году обязательно абсолютно для всех, чья работа связана с опасными производственными объектами. В данную категорию входят не только руководители и сотрудники ОПО, но и проектировщики, строители, а также те, кто занимается, ремонтом, консервацией и восстановлением ОПО.

С 01.01.2021 г. начал действовать новый алгоритм лицензирования деятельности промышленной безопасности. По новым правилам Ростехнадзор будет проверять документацию на само производство, здания, где оно функционирует, действующие на нем техустройства [4].

Дополнились требования тремя пунктами:

1. В штате организации должно работать на постоянной основе не менее трех экспертов по промышленной безопасности в 2020 году.

2. Здания, в которых осуществляется производственная деятельность ОПО, должны находиться в собственности у лицензиата или соискателя.

3. Наличие результатов экспертной проверки промышленной безопасности.

Все нововведения приняты с целью повышения безопасности работы производств, повышения качества их работы, улучшения контроля со стороны государства[5].

Совершенствование системы обучения для аттестации работников по промышленной безопасности «СИБИНТЕК»

Федеральный закон «О промышленной безопасности опасных производственных объектов» вводит определение специалиста по промышленной безопасности и уточняет, что таковым может считаться только человек прошедший обучение и подтвердивший свою квалификацию.

В настоящее время идет процесс разработки профессиональных стандартов для специалистов по промышленной безопасности. Переход к независимой системе оценки квалификации позволит улучшить качество оценки специалистов и повысить их профессиональный уровень [1].

ООО ИК «СИБИНТЕК» работает на рынке ИТ-сервиса и аутсорсинга с 1999 года и является одним из лидеров отрасли. Постоянными клиентами являются крупнейшие предприятия нефтегазовой отрасли, государственных структур, финансово-банковского сектора, розничного бизнеса.

В компании установлены высокие стандарты качества. От всех сотрудников, в том числе и от молодых специалистов, компания ожидает серьезного и ответственного отношения к работе, взамен предлагает хороший шанс развития своих профессиональных и управленческих компетенций, а также интересную работу и вывод своей карьеры на качественно новый уровень.

В компании функционирует система внутреннего обучения и институт внутренних тренеров. Основными направлениями обучения являются профессионально-техническое обучение, обязательное обучение для соблюдения стандартов работы, развитие руководителей разного уровня, программа обучения для молодых специалистов и наставников, ИТ-специалистов, рабочих, а также внутренняя годовая программа для тренеров. Обучение проходит в разных форматах от очных встреч до электронных курсов для обеспечения непрерывного развития работников.

В первые месяцы работы для каждого сотрудника организованы адаптационные тренинги, в большом объеме представлены адаптационные материалы, в которых содержится вся необходимая информация о компании, даны ответы на многие важные вопросы и полезные рекомендации для скорейшей адаптации на новом месте. В компании действует трехлетняя программа развития молодых специалистов, которая позволяет раскрыть профессиональный и карьерный потенциал и включает в себя адаптационные мероприятия, развивающие тренинги и систему наставничества.

Обучение на специалиста по промбезопасности в 2021 году включает в себя общие основы промбезопасности (программа А1) и отраслевые программы Б1-Б12, включающие в себя информацию об организации системы промышленной безопасности в отдельных отраслях:

- химическая и нефтеперерабатывающая;
- нефтегазовая;
- металлургическая;
- горнорудная;

- угольная;
- маркшейдерское обеспечение горных работ;
- объекты газораспределения и газопотребления;
- оборудование, которое работает под давлением;
- подъёмные сооружения;
- транспортировка опасных веществ;
- растительное сырьё;
- взрывные работы.

С 15.02.2021 вступает в силу Приказ Ростехнадзора от 04.09.2020 N 334 "Об утверждении Перечня областей аттестации в области промышленной безопасности, по вопросам безопасности гидротехнических сооружений, безопасности в сфере электроэнергетики" (Зарегистрировано в Минюсте России 03.02.2021 N 62362).

В соответствии с ним, с 15.02.2021 большинство областей аттестации по промышленной безопасности изменяют свое наименование (шифр), часть областей аттестации отменены, а часть объединены или введены впервые.

Соответственно, теперь для идентификации нужной области аттестации не достаточно, как это было раньше, использовать только шифр, например, Б.1.3, Б.1.8… Теперь, во избежание ошибки, необходимо полностью прописывать и проговаривать полное наименование.

Так как, например, под шифром Б.1.3 ранее была область: «Б.1.3. Эксплуатация объектов нефтехимии», а теперь, в новом перечне, «Б.1.3. Эксплуатация опасных производственных объектов сжиженного газа»… Нет больше всем известной области «Б.9.31 Эксплуатация опасных производственных объектов, на которых применяются подъемные сооружения, предназначенные для подъема и перемещения грузов», теперь вместо нее будет существовать область «Б.9.3. Эксплуатация опасных производственных объектов, на которых применяются подъемные сооружения, предназначенные для подъема и перемещения грузов». Та же участь постигла всем известную ранее под шифром Б.8.23 область «Эксплуатация сосудов, работающих под давлением, на опасных производственных объектах» – теперь, вместо нее, появляется область «Б.8.3. Эксплуатация опасных производственных объектов, на которых используются сосуды, работающие под избыточным давлением».

Заключение

В настоящее время очень популярной выступает тема организации обучения внутри организации. Огромное число руководителей осознало, что развитие персонала может выступить как некоторое из основных преимуществ компании на конкурентном рынке. Проблему безопасности в данном аспекте и рассматриваемой отрасли необходимо комплексно и систематически отслеживать. Таким образом, на сегодняшний день сформированное отношение к проблеме аварийности на промышленных объектах рассматриваемой отрасли существенно изменилось, в положительную сторону, что соответственно сказалось на снижении уровня аварийности на опасных производственных объектах как угольной так и нефтяной отрасли.

На фоне изменений ряда нормативных актов по промышленной безопасности, кроме наименований, обновляются и тесты по областям аттестации. На данный момент в системах предаттестационной подготовки по всей стране обновлена только область А.1 Основы промышленной безопасности.

Список литературы:

1. Нефтегазовая промышленность [Electronic resource]. URL: http://www.inpromservice.ru/ otrasli primeneniya/ neftegazovaya promyshlennost/ (accessed: 30.06.2021).

2. Лемента, О.Ю. Производственный травматизм как фактор снижения экономической эффективности работы горнодобывающих предприятий / О.Ю. Лемента // Экономика и управление: проблемы, тенденции, перспективы развития: материалы II Междунар. науч. – практ. конф. – Чебоксары,. – 2016. – С. 115-119.

3. Гридин, А.Д. Охрана труда и безопасность на вредных и опасных производствах / А.Д. Гридин. – М.: Альфа-Пресс, 2018. – 160 с.

4. Загутин, Д.С. Производственная безопасность / Д.С. Загутин. – М.: Русайнс, 2018. – 157 с.

5. Куракин В.И. Анализ развития нефтегазовой промышленности в Российской Федерации // Экономические науки. 2020. Vol. 12, № 193. P. 264-273.

НБ РАЗДЕЛ. ПРАВОВЫЕ И ПОЛИТИЧЕСКИЕ АСПЕКТЫ БЕЗОПАСНОСТИ

УДК 34.4414

Боярцев Михаил Сергеевич,
Волгоградского государственного университета, г. Волгоград
Boyartsev Mikhail Sergeevich, Volgograd State University, Volgograd

РОЛЬ ПРЕЗИДЕНТА РФ В ОПРЕДЕЛЕНИИ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ
ROLE OF THE PRESIDENT OF THE RUSSIAN FEDERATION IN DEFINING STATE POLICY

Аннотация: в соответствии с положениями Конституции РФ, Президент РФ самостоятельно определяет основные направления внешней политики. Эта функция вытекает из того, что он является главой государства и занимает высшую ступень в системе государственной власти и к тому же в России сложилась такая форма государственного правления, где наиболее приоритетные функции государства возлагаются на Президента РФ. Если же обратиться к юридической литературе, то функция главы государства в определении государственной политики относится к числу основных и приоритетных функций, а также выступает определяющей характеристикой его деятельности.

Absrract: in accordance with the provisions of the Constitution of the Russian Federation, the President of the Russian Federation independently determines the main directions of foreign policy. This function stems from the fact that he is the head of state and occupies the highest level in the system of state power, and, moreover, a form of state government has developed in Russia where the most priority functions of the state are assigned to the President of the Russian Federation. If we turn to the legal literature, then the function of the head of state in determining state policy is one of the main and priority functions, and is also a defining characteristic of his activities.

Ключевые слова: внешние функции государства, внутренние функции государства, государственная политика, функции главы государства, государственный совет.

Keywords: external functions of the state, internal functions of the state, state policy, functions of the head of state, state council.

Если сделать исторический экскурс, то стоит отметить важное положение – функция президента РФ в определении государственной политики оказалась случайной, так как изначально в советский период она возлагалась на Съезд народных депутатов. При разработке проекта Конституции РФ данная функция была отдана Президенту с целью демонстрации, что в России сформировано сильная президентская власть.

Государственная политика в правовой литературе именуется как особенное явление, обладающее общетеоретическим и нормативным разнообразием. К тому же, в различных зарубежных странах роль Президента РФ в определении государственной политики имеет свои характерные особенности, которые зависят в свою очередь от различных факторов. К тому же, роль главы государства в данным направлении в настоящее время возрастает, ввиду того, что в настоящее время под влиянием таких факторов как субъективных, глобальных и национальных, внутренних и внешних, происходят глобальные процессы [1, с.4]. Государ-

ственная политика государства складывается из политики социальной, политики публичной, государственно-властной. Такая политика отражает цели, задачи, направления и приоритетные направления функционирования государства как целостного социального института.

Роль Президента РФ так же возросла ввиду внесенных изменений в действующую Конституции РФ в 2020 году. Теперь же, государственная политика должна строиться таким образом, чтобы более направлением являлось развитие России как правового государства, в связи с чем, Президент РФ должен наполнять ее юридическим содержанием. Важное значение должно уделяться необходимости усовершенствовать законодательство [6, С. 306], преодолению правовых коллизий [7, С. 48]. В 2020 году глава государства отметил, что в настоящее время стоит потребность в качественном развитии всей правовой базы [2]. Из этого напрямую следует вывод, что в настоящее время государственная политика России имеет первостепенное значение и успех в ее реализации зависит прежде всего от того, как Президент РФ реализует функцию по развитию правовой базы. Главная особенность государственной политики в России состоит в том, что она является особенным средством регулирования всех сфер жизнедеятельности общества и параллельно выступает еще и механизмом средств и принципов по достижению стратегических целей и тактических задач государства и общества [3].

Президент РФ также определяет приоритетные направления государственной политики, учитывая следующие особенности:

1. Данная политика должна иметь определенные цели и задачи;
2. Как особая форма воплощения политического государства;
3. Как средство ограничения власти законом;
4. Как цель по отношению к обществу.

Стоит отметить, что также после внесения поправок в РФ был сформирован новый конституционный орган – Государственный совет, который обеспечивает согласованное функционирование и взаимодействие органов государственной власти, определяет основные направления внешней и внутренний политики государства. В связи с чем в правовом поле заговорили о том, что теперь роль Президента в данной сфере снижается, так как глава государства по факту лишился права единолично обеспечивать согласованное функционирование и взаимодействие органов государственной власти и определять основные направления внутренней и внешней политики [4]. Однако оно не является верным, так как Президент РФ не лишился функции выбора направления реализации государственной политики государства, просто эта функция также легла и на новый конституционный орган – Государственный совет, который формирует глава государства, но при этом не указано принимает ли он единоличную роль в его возглавлении.

Президент РФ также не лишился полномочий по оглашению направлений государственной политики ежегодно в специальном Послании Президента Федеральному Собранию. В 2021 году значительная часть обращения главы государства была посвящена мерам социальной поддержки. В данном направлении осуществления государственной политики прозвучало два тезиса: регионы смогут получить инфраструктурные кредиты, но только те, которые проводят взвешенную финансовую политику и также регионам были выделены бюджетные кредиты, выделенные в целях осуществления борьба с последствиями ковида [5].

Подводя итог вышесказанному стоит отметить, что функция Президента РФ в определении государственной политики основана на особенных положениях Основного закона нашего государства. Примечательно, что не во всех президентских и полупрезидентских республиках высока роль главы государства при осуществлении данной функции. Однако при этом его роль ограничена, так как его деятельность должна быть основана на конституционных положениях, посвященных внутренней и внешней политики. Хотя в Конституции РФ и закреплена данная функция государства, но закрепленные в нем пределы его полномочий размыты, так как имеются лишь общие предписания политического характера, что с одной стороны, что с одной стороны, препятствует выполнению Президентом РФ функции определения государственной политики, а с другой, увеличивает возможность производного толкования ее положений главой государства. И эта проблема может быть решены только путем внесения изменений в Конституцию РФ.

Список литературы:

1. Рудковский В.А. Основы правовой политики: учеб. пособие/ В.А. Рудковский; Федер. гос. образоват. учреждение высш. образования «Волгоград. Гос. ун-т». – Волгоград: Изд-во ВолГУ,2017. – 102 с.
2. Путин заявил о необходимости развития правовой базы в России. [электронный ресурс]. URL: https://www.gazeta.ru/social/news/2020/09/23/n_14979679.shtml
3. Парганаева Д.Н. Внутренние и внешние функции государства: исследование основных проблем // Ленинградский юридический журнал. 2018. №1 (51). URL: https://cyberleninka.ru/article/n/vnutrennie-i-vneshnie-funktsii-gosudarstva-issledovanie-osnovnyh-problem (дата обращения: 29.12.2021).
4. Гаврилов Н. П. Роль Президента Российской Федерации в определении государственной политики // ЮП. 2007. №2. URL: https://cyberleninka.ru/article/n/rol-prezidenta-rossiyskoy-federatsii-v-opredelenii-gosudarstvennoy-politiki (дата обращения: 29.12.2021).
5. Послание Президента РФ Федеральному Собранию от 21.04.2021 "Послание Президента Федеральному Собранию" // Справ. сист. Консультант Плюс
6. Боков, Ю. А. Проблемы деятельности органов государственной власти по противодействию терроризму / Ю. А. Боков, А. М. Абдуллаева // Модернизация российского общества: стратегии управления, вопросы правоприменения и подготовки кадров: материалы XX Всероссийской научной конференции (национальной с международным участием), Таганрог, 19–20 апреля 2019 года / ЧОУ ВО "Таганрогский институт управления и экономики". – Таганрог: Таганрогский институт управления и экономики, 2019. – С. 303-307.
7. Боков, Ю. А. Коллизии между федеральным и региональным законодательством: на примере Волгоградской области / Ю. А. Боков, О. Н. Мезина // Современные наукоемкие технологии. – 2005. – № 1. – С. 45-48.

Н Б РАЗДЕЛ. СОЦИАЛЬНЫЕ, ГУМАНИТАРНЫЕ И ИНФОРМАЦИОННЫЕ АСПЕКТЫ БЕЗОПАСНОСТИ

УДК 347.92
DOI 10.37539/2782-3083.2022.3.1.003

Иванова Наталия Александровна,
доцент, Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра « Экономика высокотехнологичных производств», г. Санкт-Петербург
Ivanova Natalia Aleksandrovna, Saint Petersburg State University of Aerospace Instrumentation Department of «Economics of high-tech industries», Saint-Petersburg

СИСТЕМНЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИИ
SYSTEMIC BASES FOR ENSURING THE NATIONAL SECURITY OF RUSSIA

Аннотация: в статье рассматриваются концептуальные основы экономической безопасности России, позволяющие определить общую стратегию и приоритетные направления государственной политики в области соблюдения и обеспечения экономической безопасности страны. В проведенном исследовании национальная экономическая безопасность анализируется как системное образование, в связи с чем применяются системные методологические подходы к изучению данного вопроса, выделяются основные индикаторы

уровня экономической безопасности, а также пороговые значения. В процессе исследования экономическая безопасность рассматривается как компонент национальной (государственной) безопасности. Обосновывается обеспечение национальной независимой экономики, ее стабильности и устойчивости, способности к постоянному обновлению и самосовершенствованию на основе экономических методов и средств неэкономического характера.

Abstract: the article examines the conceptual foundations of Russia's economic security, which make it possible to determine the general strategy and priority directions of state policy in the field of observing and ensuring the country's economic security. In this study, national economic security is analyzed as a systemic formation, in connection with which systemic methodological approaches are applied to the study of this issue, the main indicators of the level of economic security, as well as threshold values, are highlighted. In the process of research, economic security is considered as a component of national (state) security. The provision of the national independent economy, its stability and sustainability, the ability to constant renewal and self-improvement on the basis of economic methods and non-economic means are substantiated.

Ключевые слова: безопасность, экономическая безопасность, устойчивость, стабильность.

Keywords: security, economic security, sustainability, stability.

В мировой экономической мысли экономическая безопасность традиционно рассматривается как важнейшая качественная характеристика экономической системы, которая определяет ее способность:

- поддерживать нормальные условий жизнедеятельности населения;
- устойчиво обеспечивать ресурсам^ развитие народного хозяйства;
- последовательно реализовывать национально-государственные интересы.

Состояние национальной экономики является не просто одной из важнейших составляющих системы государственных интересов, а представляет собой решающее условие соблюдения и реализации как государственных национальных, так и общественных интересов страны. По этой причине в достаточном уровне экономики должны быть заинтересованы и государственные структуры, и частный бизнес, и все слои общества. В этих обстоятельствах экономическая безопасность конкретной личности, общества и в целом государства выражается в определенных интересах.

В настоящее время в отечественной экономической теории и практике отсутствует четкий подход к оценке экономической безопасности РФ в целом и отдельных регионов [1].

В частности, до сих пор не определены и не решены:

- минимальный информативный набор индикаторов-показателей экономической безопасности;
- пороговые значения индикаторов-показателей экономической безопасности;
- методологические проблемы прогноза динамики индикаторов – показателей экономической безопасности в средне- и долгосрочной перспективе.

Проблема экономической безопасности в зарубежной литературе рассматривается достаточно давно.

В развитых странах обеспечение экономической безопасности является приоритетным направлением государственной политики, что вызвано пониманием экономической безопасности как безусловной гарантии на уровнях:

- внешней политики – суверенитета государства;
- внутренней политики – социально-политической стабильности общества.

Традиционно теоретико-концептуальная разработка понятия “экономическая безопасность” осуществлялась в рамках ведущих научных зарубежных школ [2].

В научной литературе экономическая безопасность рассматривается как:

1. Единый, неделимый подвид рациональной безопасности. Подобный взгляд отражен у П.Г. Белова, который формулирует “...принципы не частных безопасностей, а единственно возможной – системной безопасности”.

2. Самостоятельная, автономная система в рамках национальной безопасности. В этом плане данная проблема рассматривается в двух аспектах:

• экономическая безопасность как защищенность самой экономики от воздействия различных факторов и угроз. “Экономическая безопасность означает надежную и обеспеченную всеми необходимыми средствами и интересами государственно-национальных интересов в сфере экономики от внутренних и внешних угроз, экономических и материальных ущербов”;

• экономическая безопасность как) состояние, при котором соблюдаются ее определенные пороговые критические значения.

Экономическую безопасность можно понимать как состояние готовности и возможности экономики обеспечить социально-экономическую и военно-политическую стабильность общества, государства и устойчивость экономического и правового положения каждого члена общества,

В исследованиях проблемы национальной безопасности существуют различные концептуальные подходы, выделяющие различные подсистемы, элементы и факторы национальной безопасности.

По мнению Г.В. Коржова национальная безопасность объединяет следующие подсистемы: экономическую, политическую, общественную, экологическую, технологическую, военно-техническую, информационную, психологическую (в т.ч. социально-психологическую).

Второй подход отражает концепция С.Ю. Глазьева, выделяющего военную, техническую, экономическую, социальную и научно-техническую формы.

Другие исследования, подчеркивая многоуровневость национальной безопасности, детализируют ее по предметно-функциональной направленности и выделяют военную, социальную, политическую, экономическую, экологическую, информационную, культурную, правовую, научно-технологическую, демографическую, генетическую, криминогенную, энергетическую, интеллектуальную [3].

Система национальной безопасности образуется политической, экономической, общественной (социально-психологической), военно-технической и экологической формами.

Если национальную безопасность понимать как состояние защищенности государства от внешних и внутренних угроз, при котором обеспечиваемся независимость и территориальная целостность государства, сохраняется социально-политическая стабильность и создаются условия для развития эволюционных общественных процессов, то приоритетное направление обеспечения национальной безопасности отводится ее экономической составляющей.

В методологической плане экономическая безопасность должна рассматриваться в двух аспектах при:

• устойчивом и стабильном развитии экономики;

• возникновении угроз экономической безопасности в кризисный период.

К числу основных направлений экономической безопасности относятся:

• топливно-энергетическая независимость и технологическая безопасность,

• рационализация структуры экспорта и импорта,

• создание импортозамещающих производств,

• ограничение и ликвидация организованной преступности,

• легализация теневой экономики и др.

Национальная экономическая безопасность определяется эффективным взаимодействием функционирующих экономических субъектов, влияющим на способность экономической системы выполнять свои функции.

Экономическая безопасность, а также эффективность экономики зависят от наличия “петли обратной связи” между государством, обществом и экономикой, в условиях которой деятельность общественных социально- политических институтов и институтов управления (власти) устойчиво взаиморегулируется и воспринимается! как естественный процесс на основе высокой социально-экономической организации общества [4].

В. Сенчагов считает, что безопасность представляет собой состояние объект в системе его связей с точки зрения способности к самовыживанию в условиях внутренних и внешних угроз, а также действия непредсказуемых и труднопрогнозируемых факторов.

Чем более устойчивы экономическая система (например, межотраслевая структура), соотношение производственного и финансово-банковского капитала и т.д., тем жизнеспособнее экономика, а значит, и оценка ее безопасности будет достаточно высокой. Нарушение пропорций и связей между разными компонентами системы ведет к дестабилизации и является сигналом перехода экономики от безопасного состояния к опасному.

Сущность экономической безопасности реализуется в системе индикаторов-показателей.

Совокупность индикаторов-показателей экономической безопасности – это оценка состояния экономики с позиции важнейших процессов, отражающих сущность экономической безопасности.

Индикативная оценка экономической безопасности включает в себя оценки:

• ресурсного потенциала и возможностей его развития;

• уровня эффективности использования ресурсов, капитала и труда и его соответствия уровню в наиболее развитых и передовых странах, а также уровню, при котором угрозы внешнего и внутреннего характера сводятся к минимуму;

• конкурентоспособности экономики;

• целостности территории и экономического пространства;

• суверенитета, независимости и возможности противостояния внешним угрозам, социальной стабильности и условий предотвращения и разрешения социальных конфликтов.

Стремительность возникновения очагов кризиса на отдельных территориях требует создания системы непрерывного мониторинга, которая представляла бы анализ уровня угроз экономической безопасности.

Список литературы:

1. Алексеев М.Д. Угрозы обеспечения экономической безопасности РФ / М.Д. Алексеев // Вестник НИЦ МИСИ: актуальные вопросы современной науки. – 2018. – № 5. – С. 18-26.

2. Дмитренко А.В. О концепции экологической безопасности / А.В. Дмитриенко // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. – 2019. – № 9 (112). – С. 75-78.

3. Макарейко Н.В. Экономическая безопасность в системе национальной безопасности / Н.В. Макарейко // На страже экономики. – 2020. – № 2 (13). – С. 74-80

4. Масальский М.Г., Андреев Г.О. Экономическая безопасность в современной системе международной экономической безопасности / М.Г. Масальский, Г.О. Андреев // Форум молодых ученых. – 2020. – № 10 (50). – С. 428-432.

НБ РАЗДЕЛ.
ТРАНСНАЦИОНАЛЬНЫЕ, КУЛЬТУРНЫЕ И МЕЖКУЛЬТУРНЫЕ АСПЕКТЫ БЕЗОПАСНОСТИ

УДК 34

Соломонова Виктория Валерьевна,
Воронежский экономико-правовой институт, г. Воронеж
Solomonova Victoria Valeryevna, Voronezh Institute of Economics and Law, Voronezh

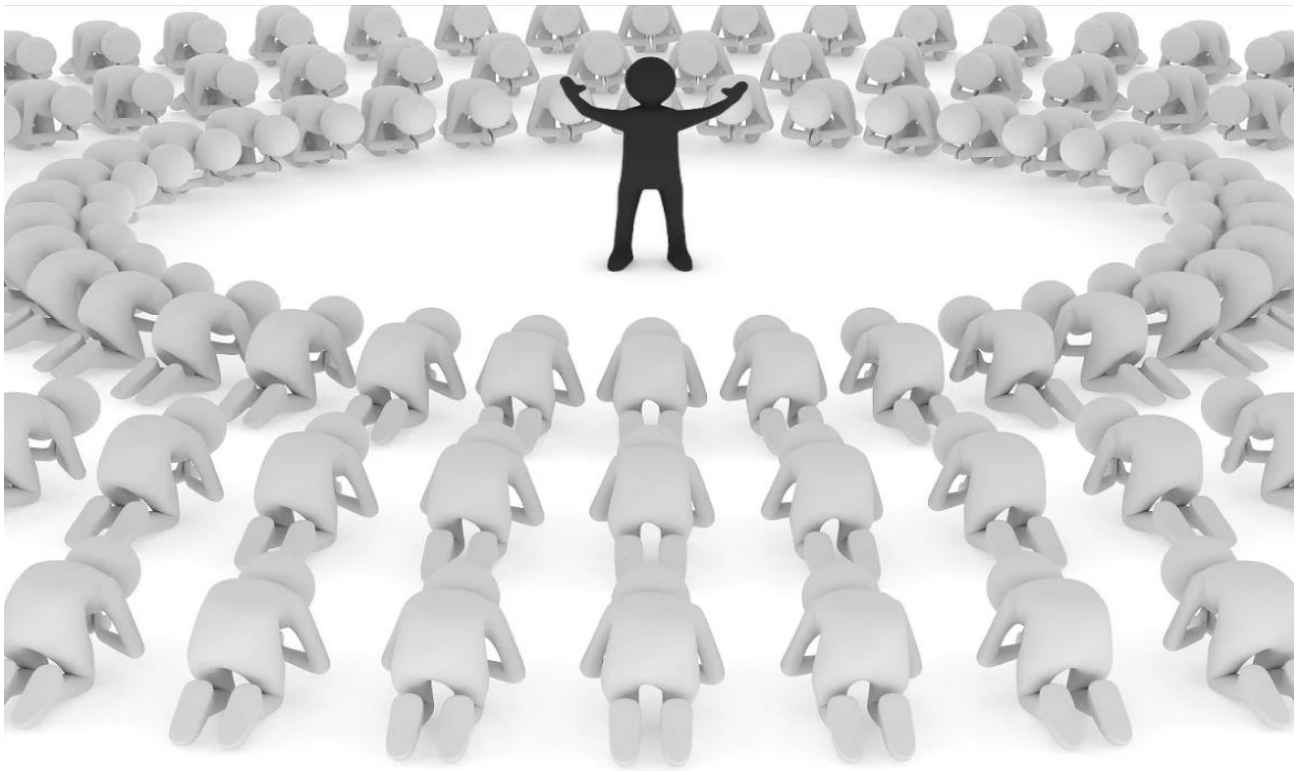
«СВИДЕТЕЛИ ИЕГОВЫ»: РЕЛИГИОЗНАЯ ОРГАНИЗАЦИЯ ИЛИ МАСШТАБНАЯ СЕКТА?
JEHOVAH'S WITNESSES: A RELIGIOUS ORGANIZATION OR A LARGE-SCALE SECT?

Аннотация: в данной статье рассматривается международная религиозная организация «Свидетели Иеговы» как запрещенное сектантское формирование.

Abstract: this article examines the international religious organization "Jehovah's Witnesses" as a banned sectarian formation.

Ключевые слова: «Свидетели Иеговы», экстремизм, государственная безопасность.

Keywords: «Jehovah's Witnesses», extremism, state security.



«Свидетели Иеговы» (иеговисты) – международная религиозная организация с численность более 8,5 млн. проповедников. Верят и поклоняются «Свидетели» единому Богу – Иегове, а также верят в противника небесных сил, олицетворяющего зло – Сатану. Суть деятельности «Свидетелей Иеговы» заключается в отвержении окружающего мира, то есть отвержение его части, где царит зло и власть не от Бога – мирская. Частично иеговисты соблюдают законы государства, они нейтрально относятся к политике, отрицательно к военной службе, а женитьба или замужество предусмотрена на человеке одной веры или на том, кто её в дальнейшем примет. «Свидетели» верят в Армагеддон, и имеют о нём представ-

ление как о сражение Иеговы и Сатаны, в ходе которого будут уничтожены только злые, плохие люди, а после Армагеддона останутся жить только те, кто служит Иегове. Таким образом, на планете не останется всяческого зла, корысти и лжи. Воскреснут не только «праведные» (верно служившие Иегове), но и «неправедные» (ослеплённые Сатаной и потому ничего не знавшие об Иегове).

История возникновения иеговистов началась с 1870 г., а именно с небольшого общества под названием «Исследователи Библии», основателем которого является Чарльз Тейз Расселл. Уже к 1877 г. «Исследователи» (в последующем «Свидетели Иеговы») проникают на территорию Российской империи[1].

«Свидетели Иеговы» проследовали свой длительный путь и до наших дней. На своей родине в США иеговисты существуют до сих пор и несут свои учения в массы, также как и в других некоторых странах. Но какое отношение к этой религиозной организации в России?

В советское время численность участников религиозной организации «Свидетели Иеговы» активно росла и распространялась по территории СССР. Деятельность иеговистов была направлена на отрицание государственной власти, что не могло не заинтересовать государственную безопасность страны. Разработка религиозных формирований госбезопасностью проводилась длительное время, о чем в феврале 1951 года было доложено МГБ СССР И. В. Сталину под грифом «совершенно секретно».

№ 194

Докладная записка МГБ СССР И.В.Сталину о необходимости выселения из западных областей Украины и Белоруссии, Молдавской, Латвийской, Литовской и Эстонской ССР участников антисоветской секты иеговистов и членов их семей

19 февраля 1951 г.
Совершенно секретно

Сталину И.В.

Докладываю, что органами МГБ в течение 1947—1950-х годов было вскрыто и ликвидировано несколько антисоветских организаций и групп нелегальной секты иеговистов, проводивших активную вражескую работу в западных областях Украины и Белоруссии, в Молдавии и прибалтийских республиках.

За это время было арестовано 1048 чел. главарей и активистов секты, изъято 5 подпольных типографий и свыше 35 000 экз. листовок, брошюр, журналов и др. иеговистской литературы.

Однако, оставшиеся на свободе сектанты-нелегалы продолжают вести активную антисоветскую работу и вновь предпринимают меры к укреплению секты.

Участники иеговистского подполья проводят злобную антисоветскую агитацию, распространяют провокационные измышления о советской власти и ведут пропаганду об установлении в СССР теократического строя, при котором власть должна принадлежать духовенству. Иеговисты выступают против мероприятий партии и советского правительства, особенно по колхозному строительству, призывают к отказу от службы в Советской Армии, распространяют среди населения антисоветскую литературу и вербуют в секту новых участников.

По агентурно-следственным материалам устанавливается, что вражеская деятельность секты иеговистов направляется Всемирным иеговистским центром в Бруклине (США) (справка о секте иеговистов прилагается).

Органами МГБ Украины, Белоруссии, Молдавии, Латвии, Литвы и Эстонии выявлено свыше 300 чел. руководящего актива иеговистов, в т.ч. 13 руководителей областных иеговистских организаций, 40 руководителей районных организаций и 250 руководителей сектантских ячеек и иеговистов.

В целях пресечения дальнейших антисоветских действий иеговистского подполья МГБ СССР считает необходимым, наряду с арестом руководящих участников иеговистской секты, выселить из пределов Украины, Белоруссии, Молдавии, Латвии, Литвы и Эстонии выявленных иеговистов с семьями в Иркутскую и Томскую обл. Всего выселению подлежит 8576 чел. (3048 семей), из них:

По Украинской ССР	— 6140 чел. (2020 семей)
По Белорусской ССР	— 394 чел. (153 семьи)
По Молдавской ССР	— 1675 чел. (670 семей)
По Латвийской ССР	— 52 чел. (27 семей)
По Литовской ССР	— 76 чел. (48 семей)
По Эстонской ССР	— 250 чел. (130 семей)

Секретарь ЦК КП(б) Украины т. Мельников, секретарь ЦК КП(б) Белоруссии т. Патоличев, секретарь ЦК КП(б) Молдавии т. Брежнев, секретарь КП(б) Латвии т. Калиберзин, секретарь ЦК КП(б) т.Снечкус и секретарь ЦК КП(б) Эстонии т. Кэбин также считают необходимым выселение иеговистов и этот вопрос с ними согласован.

Проект постановления Совета Министров по указанному вопросу при этом представляю[135].

Прошу Вашего решения.

Абакумов

АП РФ. Ф. 3. Оп. 58. Д. 180. Л. 52—53.

ИСТОРИЧЕСКИЙ ДОКУМЕНТ, ОПУБЛИКОВАННЫЙ РОССИЙСКИМ ИСТОРИЧЕСКИМ ОБЩЕСТВОМ (АП РФ.Ф.3.ОП.58.Д.180.Л.52-53).

Так, уже в апреле 1951 года сотрудниками МГБ СССР была проведена операция под кодовым названием «Север», направленная на массовое переселение иеговистов и членов их семей в Сибирь.

Только в сентябре 1965 года Указом Президиума Верховного Совета СССР были сняты ограничения по спецпоселению и освобождены из-под административного надзора органов охраны общественного порядка участники сект: «Свидетели Иеговы», «истинно-православные христиане», «иннокентьевцы», «адвентисты-реформисты» и члены их семей. Пункт второй настоящего Указа гласил, что «снятие ограничений по спецпоселению с указанных лиц не влечёт за собой возврата им имущества, конфискованного при выселении». Но, несмотря на снятие ограничений, «Свидетелей» на территории Советского союза притесняли, поскольку их подозревали в проведении активной антисоветской деятельности, направленной на изменения государственного строя СССР.

Так, в мае 1980 года Совет по делам религий принял постановление «О состоянии и мерах усиления работы по разоблачению и пресечению противозаконной деятельности секты «Свидетелей Иеговы». В период «перестройки» для иеговистов на территории СССР начался новый период – период свободы. Получив реальное право на существование, иеговисты перестали скрываться и начали открытую религиозную деятельность. Исходя из этого, произошло пополнение уже существующих собраний, а также были созданы новые, не только в крупных городах, но и в небольших, а также в деревнях и сёлах – от Москвы до Владивостока. Их членами являлись лица разной национальности, а также разных социальных и возрастных групп.

Постепенно количество иеговистов возрастало, и к 2001 г. их число на территории России превышало 250 тыс. человек! «Свидетели» выпускали массовым тиражом новую Библию и распространяли её совершенно бесплатно всем желающим, а также раздавали в оживленных местах города для привлечения новых последователей. Более того, сооружались и реконструировались специальные помещения (Залы Царства «Свидетелей Иеговы») для проведения встреч (служений) членов собраний и последователей, проводились разномасштабные конгрессы.

Так было и могло продолжаться, но 2017 год стал решающим для российских иеговистов.

20 апреля 2017 года решением Верховного Суда РФ N АКПИ17-238 было принято решение удовлетворить исковое заявление Министерства юстиции РФ и ликвидировать религиозную организацию «Управленческий центр «Свидетелей Иеговы» в России», а имущество конфисковать и обратить в доход РФ [2] .

Несмотря на то, что законодательная точка была поставлена, иеговисты продолжили свое дело, но уже в новом ключе – в подпольной законспирированной деятельности. В последующем, такие подпольные ячейки разрабатывались и пресекались сотрудниками ФСБ России, но масштабная спецоперация против «Свидетелей Иеговы» была проведена в 2020 году.

В ноябре 2020 года в Москве и еще более чем в 20 регионах России, сотрудники ФСБ провели масштабную спецоперацию против международной религиозной организации «Свидетели Иеговы».

По предварительным данным иеговисты проводили встречи в конспиративных квартирах, где изучалась, а в последующем распространялась религиозная литература, а также велась работа по вербовке новых членов. В ходе обысков были обнаружены агитационные брошюры, религиозная литература, где пропагандировалось превосходство прихожан над другими людьми, а также крупные денежные средства, которые несли последователи в качестве пожертвования.

«Свидетели Иеговы» продолжают вербовать новых участников, и если ранее вербовка происходила более открыто, то сейчас подобные действия проводятся скрытым путем, которые направлены точечно в зависимости от жизненной ситуации человека, с которым работает вербовщик. Люди жертвуют во имя спасения крупные денежные суммы, недвижимость. Пожертвования в виде ежемесячных взносов, как правило, добровольное и не фиксированное – «сколько душа подскажет», но зачастую с «душой» всесторонне «работали» через психологическое внушение пропаганды.

Экстремизм активно распространяется, имея разную направленность и виды: религиозный, национальный, политический. Правоохранительными органами ежедневно проводится ряд мероприятий по противодействию и профилактике экстремизма.

Так, 29 мая 2020 года Владимир Владимирович Путин Указом Президента Российской Федерации № 344 утвердил новую редакцию Стратегии противодействия экстремизму «Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года».

«Экстремизм является одной из наиболее сложных проблем современного российского общества, что связанно в первую очередь с многообразием его проявлений, неоднородным составов экстремистских организаций, деятельность которых угрожает национальной безопасности Российской Федерации», – говорится в Стратегии.

Оценка эффективности Стратегии будет вестись по нескольким критериям, в том числе по уровню снижения количества экстремистских угроз на территории Российской Федерации и недопущения распространения экстремистских материалов в Сети [3].

Список литературы:

1. Российские свидетели Иеговы: история и современность / Н.С. Гордиенко, СПб., 2002, С. – 233;

2. Решение Верховного Суда РФ от 20 апреля 2017 г. N АКПИ17-238;

3. Указ Президента РФ от 29 мая 2020 г. № 344 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года».

НБ РАЗДЕЛ. ЭКОЛОГИЧЕСКИЕ И БИОЛОГИЧЕСКИЕ АСПЕКТЫ БЕЗОПАСНОСТИ

УДК 636

Шишкина Мария Сергеевна, Лях Анна Викторовна,
Российский университет транспорта, г. Москва
Shishkina Maria Sergeevna, Lyakh Anna Viktorovna,
Russian University of Transport, Moscow

Королева Анна Михайловна, доцент, к.т.н.,
Российский университет транспорта, г. Москва
Koroleva Anna Mikhailovna, Russian University of Transport, Moscow

ЗАВИСИМОСТЬ – УГРОЗА ЗДОРОВЬЮ ЧЕЛОВЕКА
ADDICTION IS A THREAT TO HUMAN HEALTH

Аннотация: в данной статье затрагивается тема угрозы здоровью от зависимостей. Раскрываются последствия такого образа жизни. Химические зависимости очень пагубно и необратимо влияют на жизни людей. Разрушаются семьи, портится здоровье, жизнь делится на «до» и «после».

Abstract: this article touches on the topic of health threats from addictions. The consequences of such a lifestyle are revealed. Chemical addictions have a very detrimental and irreversible effect on people's lives. Families are destroyed, health deteriorates, life is divided into "before" and "after".

Ключевые слова: зависимость, наркотики, алкоголь, табак, здоровье.

Keywords: addiction, drugs, alcohol, tobacco, health.

Реальность такова, что на человеческую долю выпадает множество трудностей и невзгод. Каждый по-своему справляется с проблемами и, к сожалению, есть губительные пути, такие как различные зависимости. Однако не всегда человек приобретает какую-либо зависимость в результате жизненных потрясений и трудностей.

Зависимость – это патологическая потребность в чем-либо, навязчивое влечение. Человек стремится к тому, что доставляет ему удовольствие. Желание наполнить свою жизнь удовольствием – общая черта, объединяющая людей, склонных к различным зависимостям.

Ежегодно появляются новые формы зависимости. В целом зависимости могут быть:

• системные (охватывающие все отношения личности) – элементарные: наркомания, алкоголизм, фанатизм – спортивная, ургентная, запойное чтение и др.;

• осознанные (спортивная) – неосознаваемые (религиозная, наркотическая);

• социально одобряемые (трудоголизм, спортивная) – неодобряемые (токсикомания, наркомания);

• химические (наркомания, алкоголизм) – нехимические (пищевая, игровая зависимость);

• психические – физические.

К нехимическим аддикциям относят: гемблинг, любовную аддикцию, шопоголизм, ургентную аддикцию, трудоголизм, булимию, анорексию, спортивную аддикцию и многие другие [1].

В данной статье я хотела бы затронуть зависимости, которые напрямую пагубно влияют на здоровье человека. Пьянство также потребление наркотиков стали без сомнения «национальным бедствием». Стремительно нарастая во 1990-е гг., употребление спиртного, различных наркотиков, летучих ингалянтов, начиная примерно с 2002-2003 гг., приостановилось и стабилизировалось, но до сих пор тенденция к уменьшению их потребления

несерьезна либо мало видна. Потребление абсолютно всех вышеуказанных веществ наступает в подростковом возрасте, несколько реже в младшем. Результаты употребления наркотиков, токсических веществ или же злоупотребления спиртным в раннем возрасте при небольших вариациях однотипны: потеря здоровых интересов, сокращение умственных возможностей, разрушение молодых семей. Зависимость от спиртного либо наркотиков – это большой удар по обществу и бороться с этим необходимо работой среди молодого поколения в школах, училищах, институтах, университетах [2, с 6].

Психологическая зависимость: стремление к приему психоактивных средств, без существенного физического дискомфорта вне их приема (это первая фаза, а иногда единственная фаза развития зависимости).

Физическая зависимость: прием психоактивных средств с возникновением тяжелых расстройств вне их приема (вторая фаза развития зависимости). Эти расстройства объединяются в «синдром отмены»: тяжелые болевые ощущения, упадок настроения, сердечно-сосудистые, желудочно-кишечные и другие расстройства вне приема наркотиков. При алкоголизме еще в ходу термин «синдром похмелья».

Наркомания – употребление с образованием зависимости психоактивных веществ, относящихся к списку наркотиков

Токсикомания – употребление с образованием зависимости от веществ, не относящихся к списку наркотиков [2, с. 8].

Смертность в России от причин, связанных с наркотиками, в прошлом году выросла на 60%, до 7316 человек (в прошлом году умерло 4569).

Росстат включает в категорию смертности от наркотиков:

Умерших от психических расстройств в результате злоупотребления наркотиками;

Умерших от случайного отравления наркотиками или галлюциногенами, а также от отравления наркотиками «с неопределенными намерениями, не классифицированного в других рубриках» [3].

Наркотическая, алкогольная и табачная зависимость сильно влияет на здоровье человека. Алкоголь уничтожает клетки печени, а ведь в ней происходит образование АТФ (аденозинтрифосфорной кислоты – основного источника энергии в организме), детоксикация (обезвреживание) ядов и многое другое. Алкоголь особенно вреден для растущего организма. Те дозы, которые являются приемлемыми для взрослого, для молодых людей могут стать смертельными. Алкогольная интоксикация наступает у них чаще и быстрее. При поражении головного мозга могут произойти необратимые явления, способные привести к инвалидности и смерти. Злоупотребление алкоголем ведет к деградации личности, делает человека психически неуравновешенным. 70% преступлений против личности совершается в состоянии алкогольного опьянения. Это наиболее тяжелые социальные последствия алкогольной зависимости.

Табакокурение относят к вредным привычкам, которые являются отклонениями от здорового образа жизни. Проблема курения в России имеет характер национального бедствия и грозит будущему общества в целом. Сейчас юноши и девушки начинают курить в 13, 15, 17 лет и к детородному возрасту практически около 90% юношей и 40% девушек употребляют табак. У начинающего курильщика в течение 2-3 лет истощаются запасы психической энергии, поэтому у курящих юношей и девушек, вступающих в брак, не могут родиться здоровые дети (особенно в условиях общей неблагоприятной экологической обстановки).

Большинство людей, страдающих от проблем, вызванных употреблением наркотиков, считают, что достаточно прекратить их употребление и жизнь наладится. Здесь и проявляется основной парадокс химической зависимости: чтобы восстановить свою жизнь и выздороветь, необходимо оставаться чистым и трезвым, а сами повреждения, вызванные употреблением наркотиков, не позволяют вести такой образ жизни. Наиболее частые последствия употребления наркотиков для физического здоровья – это заболевания сердечно-сосудистой системы и дыхательных путей, гепатиты и цирроз печени, психозы, эпилепсии и др. Развиваются депрессии, чувства вины, бессилия, безысходности, обиды и негодования. Нарушаются духовные качества: появляется апатия, потеря смысла жизни, человек начинает

ощущать враждебность окружающего мира. Социальные последствия наркомании – это зависимость наркомана от продавца наркотиков, добывание денег не трудовым, а иногда и вовсе преступным путем. Наркомания, проституция, убийства, грабежи, СПИД – вот единый антисоциальный клубок. Лечение наркоманов и содержание их больных детей – тяжелая социальная ноша. Причем лечение наркомании – процесс долгий и дорогой.

Таким образом, химические зависимости очень пагубно и необратимо влияют на жизни людей. Разрушаются семьи, портится здоровье, жизнь делится на «до» и «после».

Список литературы:

1. Кутбиддинова, Р.А. Психология зависимости: учебно-методическое пособие / Р.А. Кутбиддинова. – Южно-Сахалинск: СахГУ, 2017 с 9-10

2. Спринц А.М., Ерышев О.Ф. Химические и нехимические зависимости / А.М. Спринц, О.Ф. Ерышев. – СПб.: СпецЛит, 2012. – 127с.

3. Федеральная служба государственной статистики [Электронный ресурс]. Режим доступа https://rosstat.gov.ru/

УДК 636

Агафонов Михаил Артемович, Шадыев Рустам Русланович,
Российский университет транспорта, г. Москва
Agafonov Mikhail Artemovich, Shadyev Rustam Ruslanovich,
Russian University of Transport, Moscow

Королева Анна Михайловна, доцент, к.т.н.,
Российский университет транспорта, г. Москва
Koroleva Anna Mikhailovna, Russian University of Transport, Moscow

ВЛИЯНИЕ СОСТОЯНИЯ БИОСФЕРЫ НА ЗДОРОВЬЕ ЧЕЛОВЕКА
THE IMPACT OF THE STATE OF THE BIOSPHERE ON HUMAN HEALTH

Аннотация: в статье затрагиваются экологические проблемы, оказывающие влияние на здоровье современного человека. Человечество, стремясь улучшить условия своей жизни, непоправимо испортило окружающую среду. Проблема экологии – одна из самых актуальных в наше время, и хочется верить, что наши потомки не будут так подвержены негативным факторам окружающей среды, как мы сейчас.

Abstract: the article deals with environmental problems affecting the health of modern man. Humanity, striving to improve its living conditions, has irreparably spoiled the environment. The problem of ecology is one of the most urgent in our time, and I want to believe that our descendants will not be as exposed to negative environmental factors as we are now.

Ключевые слова: экология, биосфера, здоровье, окружающая среда, природные ресурсы.

Keywords: ecology, biosphere, health, environment, natural resources.

Современная биосфера представляет собой сложную экосистему, состоящую из многих компонентов, включающих всю живую и часть неживой природы. Все процессы в биосфере взаимосвязаны. Человечество – лишь незначительная часть биосферы, а человек является только одним из видов органической жизни. Биосферу изучает глобальная экология.

Экология – это общепризнанная наука. Поначалу экология изучала связи между растениями и животными. Современная экология рассматривает также воздействие человека на окружающую среду, влияние предприятий на биосферу. Человек сосредоточивает в себе взаимодействие природного и социального начал. Следовательно, для человека окружающая среда – это совокупность как естественных, так и социальных систем, в которых он существует. Экология – это наука об отношениях растительных и животных организмов и образуемых ими сообществ между собой и с окружающей средой [1].

Воздействие экологических факторов на состояние здоровья населения является одной из актуальнейших проблем современности. На значимость данной трудности для современного населения бесспорно указывают результаты социологического опроса, в ходе которого были получены следующие результаты: 47,2% анкетированных ответили, что их тревожит экологическое положение в местах их проживания, в то же время 29,4% ответили более расплывчато «скорее тревожит, чем нет», еще 13,7% ответили «скорее не тревожит», а 4,6% затруднились ответить на вопрос. И только 5,3% однозначно дали ответ «не тревожит» [2]. Беспокойство людей на этот счет в первую очередь связано с тем, что наблюдается изменение «традиционных» форм болезней и появление новых.

Понятие «здоровье человека», включает состояние полного физического душевного, социального благополучия, а не исключительно отсутствие болезни физиологических повреждений человека. Подобный подход учитывает, в какой мере окружающая человека среда способствует сохранению здоровья, предотвращению болезней, обеспечивает нормальные условия труда и быта, развитие. В связи с этим здоровье человека чаще всего именуют критерием оценки, показателем качества жизни.

Так, согласно статистическим данным Министерства здравоохранения РФ в 2016 г. на территории Российской Федерации зафиксировано 678425 человек с заболеваниями верхних дыхательных путей, почти 300 тысяч человек с сердечно-сосудистыми нарушениями разной степени тяжести. Сведения о более 600 тысяч человек с психическими расстройствами, в первую очередь выражающимися посредством расстройства поведения, также говорят об ухудшении условий существования человека. А цифра почти в 200 тысяч человек с онкологическими новообразованиями различных органов и систем лишь подчеркивают это умозаключение [3].

Кроме того, за последние несколько десятилетий резко увеличилось число нервно – психических отклонений и онкологических заболеваний. И в данном случае нельзя списать это изменение статистики только на увеличение продолжительности жизни, поскольку среди заболевших наблюдается значительное число людей зрелого и юношеского возраста.

К числу особенно крупных источников, поставляющих в окружающую среду вредоносные для здоровья человека загрязнители, причисляются предприятия черной и цветной металлургии, комплексы химических, нефте- и сланцеперерабатывающих предприятий, предприятия по выработке строительных материалов и автотранспорт.

Заметное вредоносное воздействие человека на окружающую среду началось с периода становления научно-технического прогресса. воздействие это мгновенно стало комплексным – использование агрессивных соединений в промышленности, добыча полезных ископаемых открытым методом, вмешательство в естественные экосистемы и т. п. впрочем стоит заметить, что численность человечества в то время составляла около 500 млн человек, поэтому и необходимости в материальных благах были значительно ниже [4].

Однако, с середины XX века, мы можем увидеть резкий скачок в развитии технологий и науки. Люди начинают заметно больше использовать ресурсов и полезных ископаемых и т.д., и вследствие этого происходит опустошительный эффект.

Из-за влияния транспортных средств, работы современных промышленных предприятий и энергостанций, атмосфера с каждым днем загрязняется в геометрической прогрессии. Список вредных веществ, попадающих в атмосферу, огромен – он охватывает практически всю таблицу химических элементов, которые при попадании в организм любого живого существа могут вызвать необратимые патологические изменения.

По проведенным исследованиям мы можем увидеть, что, почти 2/3 всех человеческих заболеваний на планете возникают из-за употребления обычной питьевой воды.

От употребления загрязненной воды могут быть следующие последствия:

1) развитие онкологических заболеваний;

2) снижение иммунитета человека;

3) генетические изменения, при которых рождаются дети с мутациями;

4) снижение работы детородных органов, как у женской половины, так и мужской;

5) заболевания внутренних органов, а именно печени, почек и желудочно-кишечного тракта.

С каждым годом в обычных продуктах питания, систематически употребляемых человеком, которые являются для него необходимыми и должны приносить только пользу для организма, обнаруживается все больше вредных веществ, присутствие которых крайне негативно отражается на здоровье человека. Именно по этой причине в нашей стране, да и во всем мире, появляется все больше неизлечимых заболеваний.

Подводя итог, отмечу, что проблема экологии – одна из самых актуальных в наше время, и хочется верить, что наши потомки не будут так подвержены негативным факторам окружающей среды, как мы сейчас. Человечество уже осознает сложившуюся ситуацию, что в будущем должно привести к ее решению. Однако кто знает, сколько потребуется времени, чтобы хотя бы немного приблизиться к восстановлению того, что мы испортили. Человечеству будет тяжело разорвать круг, при котором с ростом комфортных условий, загрязняется окружающая среда.

Список литературы:

1. В. А. Дерябин Экология: учебное пособие / В.А. Дерябин, Е.П. Фарафонтова. – Екатеринбург: Изд-во Урал. ун-та, 2016. – 136 с.

2. Экология и здоровье человека [Электронный ресурс]. Режим доступа: http://mirznanii.com/.

3. Степановских А.С. Экология: учебник для вузов. М.: ЮНИТИ – ДАНА, 2001. 703 с.

4. Влияние экологических факторов на здоровье человека [Электронный ресурс]. Режим доступа: http://valeologija.ru/valeologija-russkij/13/92-vliyanie-ekologicheskix-faktorov-na-zdorovecheloveka

УДК 614

Савинова Владислава Евгеньевна,
Российский университет транспорта, г. Москва
Savinova Vladislava Evgenievna, Russian University of Transport, Moscow

Королева Анна Михайловна, доцент, к.т.н.,
Российский университет транспорта, г. Москва
Koroleva Anna Mikhailovna, Russian University of Transport, Moscow

ЭФФЕКТИВНОСТЬ АНТИОБИТИКОВ В БОРЬБЕ С ВИРУСАМИ
THE ANTIBIOTICS EFFICIENCY AGAINST VIRUSES

Аннотация: на основе литературных данных в статье главным образом исследована медико-санитарная обстановка в современном обществе. С опорой на теоретические аспекты иммунологии и вирусологии доказана нерациональность употребления антибиотиков в случаях проникновения вирусов в организм человека.

Abstract: based on the literature sources, the article mainly contains the sanitary and epidemiological disquisition of situation in modern society. Based on the theoretical aspects of immunology and virology, the irrationality of the antibiotics usage in cases of virus penetration into the human body has been proven.

Ключевые слова: бактерия, вирус, иммунитет, антибиотики.

Keywords: bacteria, virus, immunity, antibiotics.

Зачастую на различных упаковках медицинских препаратов, повышающих иммунитет, мы можем увидеть надпись, гласящую о том, что данное средство помогает бороться с вирусами и бактериями в организме человека, не позволяя проникнуть в него. Тем не менее не каждый задумывается об эффективности данного лекарства, принципе его работы и даже об особенностях вирусов и бактерий.

Микроорганизмы – древнейшее царство на Земле, представители которого заселяют абсолютно каждую точку планеты. Люди для них – просто разновидность питательной среды. Стоит акцентировать внимание на **патогенах** (от греч. «Пато» – страдать, «Гено» – рождать), представляющих собой любой вид вредоносных микроорганизмов (бактерии, вирусы и т. д.) [3]. Они проникают из внешней среды в организм человека, паразитируют на наших клетках, размножаются и в целом отравляют организм. Причем одни и те же болезни могут вызвать разные микробы.

На первый взгляд кажется, что бактерии и вирусы – это одно и то же, поскольку они являются возбудителями болезней, однако существует колоссальная разница между ними.

Бактерия представляет собой одноклеточный живой организм, способный обеспечить все этапы своего жизненного цикла самостоятельно [2]. Стоит отметить, что не все бактерии вредны для человека, многие из них могут быть безопасны или даже полезны. Например, на этикетках йогуртов можно увидеть, что в состав продукта входят бифидо- и лактобактерии, которые действительно помогают нормализовать процессы в человеческом организме, в частности работу кишечника.

Вирус – это внутриклеточный паразит, не способный жить самостоятельно и состоящий из генетического материала (ДНК или РНК) и защитной оболочки [2].

Так как они не могут размножаться путем деления клеток, они используют живые клетки других организмов для создания своих копий. Изначально вирус прикрепляется к поверхности клетки-хозяина, а затем проникает в нее, высвобождая генетический материал, после чего происходит размножение. Простуду с насморком умеют создавать различные вирусы: риновирусы, коронавирусы, вирусы гриппа и т.д.

Люди постоянно чихают и кашляют, разнося огромное количество патогенов в окружающей среде, а другие заносят их внутрь, трогая глаза, нос, рот или губы. Согласно данным социального эксперимента Национального центра биотехнологической информации, в среднем каждый из 26 наблюдаемых студентов касался своего лица 23 раза в час. Стоит учитывать тот факт, что далеко не каждый человек соблюдает гигиену рук, однако в 44% случаев люди касаются именно слизистых оболочек, увеличивая риск проникновения вредных бактерий в организм [5].

После выздоровления в организме человека появляются антитела, которые нейтрализуют клетки патогенов и вирусов. То есть организм человека приспосабливается к заболеванию, становится сильнее, так как учится бороться с различными заразами. Таким образом, вырабатывается иммунитет.

Адаптивный иммунитет – тот иммунитет, который адаптируется, подстраивается под конкретного врага. Здесь речь более подробно пойдет об антителах. **Антитела** – это гликопротеины, связывающие определенные антигены и представляющие собой Y-образные белки.

Они оставляют на патогене свою метку, после чего иммунные клетки сразу же узнают врага и вступают в бой.

Проблема заключается в том, что вирусы эволюционируют, меняют свои рецепторы, из-за чего их тяжелее вычислить. Что в свою очередь делает организм? Иммунитет сам меняет местами гены для антител, чтобы они идеально подходили к любому вредоносному микроорганизму. Удивительно то, что таким образом иммунная система находит ключ к абсолютно любой заразе в мире.

Антибиотики представляют собой антимикробные препараты, которые создаются из продуктов жизнедеятельности других микробов, растений или путем искусственного синтеза. Сегодня они продаются в каждой аптеке, и здесь возникает проблема самолечения, поскольку при малейшем подозрении на инфекцию люди сразу же прописывают их сами себе. Антибиотик не может противостоять вирусу, поскольку у вируса нет клеточной стенки и аппарата для выработки белков, которые мог бы приостановить антимикробный препарат, следовательно, между ними никакого взаимодействия не произойдет [3]. Простуда возникает из-за проникновения вирусов в организм, а значит, антибиотики тут не помогут. Следовательно, главной угрозой для человечества является сам человек.

Стоит отметить, что применение антимикробных препаратов в нецелесообразных случаях только вредит здоровью, так как они уничтожают полезные бактерии, например в кишечнике, но в этом случае остаются только самые стойкие и вредные бактерии. Волна антибиотиков, пытаясь уничтожить бактерию, стимулирует её к мутациям, из-за чего она адаптируется к новому токсину, и как только это происходит, антибиотик для бактерий уже не представляет угрозы.

Тем не менее «Вирусы – двигатели эволюции». По словам кандидата биологических наук Шеховцовой Нины Валентиновны, человеческий геном также состоит из «приручённых» вирусов [1]. Кроме того, при появлении новых инфекций, порой даже масштабных, выделяются средства на разработку новых медицинских препаратов, вводятся различные ограничения, охраняемые законом. Ярким примером является обстановка с новой коронавирусной инфекцией.

Анализируя современную социально-экономическую обстановку, можно увидеть, что многие маркетологи и специалисты по рекламе пренебрегают фактом бесполезности антибиотиков против вирусов и создают рекламные кампании, нацеленные на реализацию продукта. С одной стороны, производитель, безусловно, получает прибыль, однако в то же время способствует возникновению негативных последствий для здоровья общества. К сожалению, чаще всего человек не читает инструкцию по применению медицинского препарата, поэтому даже не задумывается о его эффективности в тех или иных случаях.

Таким образом, человек, употребляя антимикробные препараты, предоставляет патогенам возможность становится сильнее, а значит, что многие вирусы, вызывающие уже побежденные человечеством болезни, могут вернуться с новыми силами, поскольку на фоне ослабленного иммунитета вирусам проникнуть в организм еще проще.

Список литературы:

1. Нина Шеховцова: «Вирус – это двигатель эволюции» // Ярославский государственный университет им. П. Г. Демидова URL: http://www.uniyar.ac.ru/news/science/nina-shekhovtsova-virus-eto-dvigatel-evolyutsii/ (дата обращения: 08.11.2021).

2. Про вирусы и бактерии: когда действительно нужен антибиотик // MEDCENTR URL: https://medcentr.dp.ua/stati/virusy-bakterii-antibiotik/ (дата обращения: 02.12.2021).

3. Microbiology by numbers // nature URL: https://www.nature.com/articles/nrmicro2644 (дата обращения: 03.12.2021).

4. Почему антибиотики бессильны против вирусов? // Наука и жизнь URL: https://www.nkj.ru/archive/articles/24629/ (дата обращения: 08.11.2021).

5. Face touching: a frequent habit that has implications for hand hygiene // PubMed.gov URL: https://pubmed.ncbi.nlm.nih.gov/25637115/ (дата обращения: 02.12.2021).

УДК 614

Савинова Владислава Евгеньевна,
Российский университет транспорта, г. Москва
Savinova Vladislava Evgenievna, Russian University of Transport, Moscow

Королева Анна Михайловна, доцент, к.т.н.,
Российский университет транспорта, г. Москва
Koroleva Anna Mikhailovna, Russian University of Transport, Moscow

АНАЛИЗ САНИТАРНО-ЭПИДЕМИОЛОГИЧЕСКОЙ ОБСТАНОВКИ В ОБЩЕСТВЕ В 2021 ГОДУ
ANALYSIS OF THE SANITARY AND EPIDEMIOLOGICAL SITUATION IN SOCIETY IN 2021

Аннотация: на основе литературных данных в статье исследована санитарно-эпидемиологическая обстановка в современном обществе, рассмотрен исторический ход развития эпидемий и средств защиты. С опорой на анализ развития коронавирусной инфекции доказана актуальность вакцинации, использования средств индивидуальной защиты, соблюдения мер предосторожности.

Abstract: based on the literature data, the article examines the sanitary and epidemiological situation in modern society, examines the historical course of the development of epidemics and means of protection. Based on the analysis of the development of coronavirus infection, the relevance of vaccination, the use of personal protective equipment, and compliance with precautionary measures has been proven.

Ключевые слова: вирус, коронавирус, локдаун, средства индивидуальной защиты, ограничительные меры.

Keywords: virus, covid-19, lockdown, measures of precautious, restrictive measures.

Стоит понимать различие таких форм распространения инфекции, как эпидемия и пандемия: **эпидемия** представляет собой распространение инфекционной болезни среди людей в пределах страны, значительно превышающее обычно регистрируемый на данной территории уровень заболеваемости; если инфекция широко распространена в нескольких странах одновременно, то в таком случае это **пандемия**. Можно сказать, что пандемия – это мировая эпидемия.

В 1346 году на территории Азии вспыхнула одна из известнейших в истории эпидемий чумы, получившая название «Черная смерть».

В то время люди использовали кардинально отличавшиеся от привычных нам средства защиты, поскольку тогда наука и медицина не были развиты так, как сейчас. Например, применение запахов, перебивающих запах чумы, однако трудно судить о целесообразности такого метода, поскольку патогенов не напугают чужеродные запахи, им нужна пища в виде человеческих тканей. Однако были и традиционные методы защиты – соблюдение личной гигиены, которое остается важным и по сей день, изоляция больных. Кроме того, врачи советовали людям уезжать подальше от очагов, где вспыхивала инфекция.

Специфическими средствами защиты обладали «чумные доктора» – именно те люди, которые находились в постоянном контакте с зараженными. Они носили костюмы из кожи, пропитанной уксусом, маску, внутрь которой клались душистые травы для фильтрации вдыхаемого воздуха, имели при себе скальпель для разреза бубонов, трость для обследования и чеснок, который ели постоянно.

Пандемия оспы охватывала человечество всего один раз за всю историю, но боролись с ней сотни лет, и только в XX веке вирус этой болезни стали считать окончательно побежденным. Методами защиты от заражения были: изоляция больного, позже была найдена вакцина. В целом можно заметить, что такие методы применяются и в современной обстановке.

До разработки вакцины против оспы применялась **вариоляция** – процесс, заключающийся в прививке оспенного гноя из созревшей пустулы больного натуральной оспой, приводивший к заболеванию оспой в легкой форме. Проанализировав это, мы можем сделать вывод, что он представляет собой аналог вакцинации, но его спецификой является то, что этот процесс применялся только для профилактики оспы.

Вакцина – медицинский иммунобиологический препарат, предназначенный для приобретения организмом аддаптивного иммунитета к данному конкретному антигену. Принцип действия прививки основывается на «ознакомлении» организма с конкретным вирусом и выработкой антител.

Первая вакцина была разработана в XVIII веке доктором Дженнером, а во второй половине XX в. ВОЗ организовала программу массового оспопрививания.

В последние месяцы Первой мировой войны возникло массовое заболевание гриппом, предположительно, в Испании, которое назвали «испанкой», однако Испания была нейтральной стороной в этой войне, поэтому именно ее объявили как первый очаг заражения, поскольку остальные стороны скрывали факт распространения инфекции. В любом случае это был новый штамм, к которому организм человека не был готов.

Тенденция к массовому распространению инфекции была обусловлена отсутствием необходимых средств лечения и профилактики заболевания, способов достоверной диагностики, современного технического оборудования для обеспечения санитарно-эпидемиологического надзора.

Тем не менее люди старались предотвратить заражение, полоская рот соляным раствором, а также используя дезинфецирующие средства. Кроме того, использовались индивидуальные средства защиты – маски, которые были обязательны; закрывались общественные места. Многие способы профилактики болезни напоминают сегодняшние средства, а значит, мы можем сделать вывод, что обязательное ношение масок и перчаток в современном мире – не новое, а хорошо забытое старое.

Абсолютно новой болезнью второго десятилетия XXI века является covid-19. Коронавирусы – обширное семейство вирусов, поражающих людей и животных.

Основными симптомами являются: высокая температура, кашель, боль в мышцах, высокая утомляемость, потеря чувствительности к запахам и вкусам, головная боль, заложенность в грудной клетке, кровохаркание, тошнота, рвота.

Таким образом, в 2021 году перед миром стоит проблема разработки способов и методов борьбы с инфекционными заболеваниями, которую человечество может решить только совместно.

31 января 2020 г. было подписано постановление Правительства РФ «О внесении изменения в перечень заболеваний, представляющих опасность для окружающих», где была указана коронавирусная инфекция (2019-nCoV) [5].

25 марта 2020 года Президент РФ подписал указ «Об объявлении в Российской Федерации нерабочих дней» [4], согласно которому с 30 марта по 3 апреля 2020 г. были объявлены выходные дни для граждан, а 27 марта в Москве был введен режим тотальной изоляции, получивший название локдаун [8].

Локдаун – синоним слов «самоизоляция» и «карантин», отличающийся ограничением перемещения всех граждан РФ. Вспомнив эпидемию оспы, мы можем сделать вывод, что данный метод борьбы с распространением инфекции абсолютно не новый, однако его специфической чертой является более строгий характер.

Важно отметить то, что представители населения РФ стали негативно реагировать на такой способ борьбы, ссылаясь на ст. 27 Конституции РФ [1], но в соответствии со ст. 5 Федерального закона от 30.03.1999 №52-ФЗ «О санитарно-эпидемиологическом благополучии населения» данная мера является полностью правомерной [3].

Обязательное ношение масок и перчаток породило в обществе мнение о неэффективности данных методов защиты. Вспомним о том, что вирусы и патогены могут передаваться воздушно-капельным путем, поэтому одноразовая маска позволяет предотвратить проникновение в организм инфекций.

Во время «испанского» гриппа люди так же носили маски в общественных местах, но отличие заключалось в материале медицинского изделия – оно было сшито из нескольких слоев марли.

В соответствии со ст. 236 УК РФ лицо, нарушившее санитарно-эпидемиологические правила и повлекшее массовое заболевание, подвергается уголовной ответственности [2].

На основании приведенных положений можно сделать вывод о необходимости применения индивидуальных средств защиты, поскольку это в первую очередь предоставляет человеку возможность обезопасить себя и своих близких от заражений.

Введение российской вакцины является дискуссионным вопросом в гражданском обществе, поскольку бытует мнение о неэффективности медицинского препарата. Существуют случаи, когда люди отказывались от прививки, рассчитывая на эффективность антибиотиков, однако covid-19 – это вирус, следовательно, он не поддается действию антимикробных препаратов. Принцип действия прививки основан на формировании у вакцинированного легкой формы инфекции и, как следствие, выработке антител к конкретному антигену.

Тем не менее, анализируя влияние определенных ограничений, можно сказать о положительных результатах:

1. Введение дистанционного формата работы и учебы поспособствовало развитию цифровой среды (развитие интернет-пространства для бизнеса, образования).
2. Из-за закрытия границ начал активно развиваться внутренний туризм.
3. Осознание гражданами ценности свободы передвижения.
4. Тяжелая эпидемиологическая обстановка дала толчок в развитии медицины (разработка новых лекарственных препаратов, улучшение технического состояния оборудования).
5. Изменение отношения людей к собственному здоровью (важность соблюдения гигиены, социальной дистанции и т. п.).

История эпидемий наших предков предоставляет нам возможность выявить определенные варианты перспектив развития пандемии коронавируса:

1. Окончательная победа над инфекцией при условии достижения популяционного иммунитета, как это было с оспой.
2. Жизнь с вирусом – аналогичная ситуация с «испанкой», поскольку сезонные эпидемии гриппа существуют и в наши дни, однако у человечества есть доступ к лекарственным препаратам, помогающим предотвращать развитие тяжелой формы.
3. Возникновение других заболеваний на фоне covid-19, с которыми придется бороться, поскольку инфицированный организм может столкнуться с побочными эффектами, вызванными иными вирусами или патогенами.
4. Победа над вирусом лишь на определенный период времени, поскольку, как показывает история с эпидемией чумы, вирус мутировал и стимулировал возникновение новых масштабных заражений.

Таким образом, мы можем сделать вывод о том, что главной целью современного общества относительно эпидемиологической ситуации является достижение коллективного иммунитета не менее 80%, для чего необходимо соблюдать все предусмотренные меры, включая соблюдение социальной дистанции для сокращения вероятности передачи инфекции от одного лица к другому, ношение средств индивидуальной защиты, соблюдение гигиены, своевременную вакцинацию.

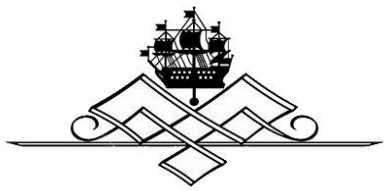
Список литературы:

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ, от 01.07.2020 №1-ФЗ) // Собрание законодательства РФ, 03.07.2020, № 31, ст. 27
2. Уголовный кодекс Российской Федерации: Федеральный закон № 63-ФЗ: [принят Государственной Думой 24 мая 1996 года: одобрен Советом Федерации 5 июня 1996 года (редакция от 27.12.2019). – URL: http://www.consultant.ru (дата обращения: 12.11.2021).

3. Закон Российской Федерации "О санитарно-эпидемиологическом благополучии населения" от 12 марта 1999 г. №52-ФЗ // Собрание законодательства Российской Федерации. 1999 г. № 14. Ст. 1650

4. Указ Президента Российской Федерации "Об объявлении в Российской Федерации нерабочих дней" от 25.03.2020 № 206 // Собрание законодательства Российской Федерации. 2020 г. № 13. Ст. 1898

5. Постановление Правительства Российской Федерации от 31.01.2020 № 66 "О внесении изменения в перечень заболеваний, представляющих опасность для окружающих" [Электронный источник] // URL: http://publication.pravo.gov.ru/Document/View/0001202002030005 (дата обращения 12.11.2021)



Ближайшие конференции
ГНИИ «НАЦРАЗВИТИЕ» (РИНЦ+DOI)

Шифр	Наименование конференции	Дата
НИТП 325	Всероссийская (национальная) научно-практическая конференция **"Научные исследования в современном мире. Теория и практика"**	10 февраля 2022 года
ФИПИ 325	Всероссийская (национальная) научная конференция **"Фундаментальные и прикладные исследования. Актуальные проблемы и достижения"**	11 февраля 2022 года
СМИН 325	Всероссийская (национальная) научная конференция **"Современные методы и инновации в науке"**	12 февраля 2022 года
ИПГС 325	Всероссийская (национальная) научно-практическая конференция **"Исследование и практика в социально-экономической и гуманитарной сфере"**	13 февраля 2022 года
SRP 301	International Scientific Conference "**Science.Research.Practice**" (Международная конференция "**Наука. Исследования. Практика**")	23 февраля 2022 года
TNS 301	International Scientific Conference "**Technical and Natural Sciences**". (Международная научная конференция "**Технические и естественные науки**")	24 февраля 2022 года
SEH 301	International Scientific Conference "**Socio-Economic Sciences & Humanities**". (Международная научная конференция "**Социально-экономические и гуманитарные науки**")	25 февраля 2022 года
ECS 301	International Scientific Conference "**Education, Culture and Society**". (Международная научная конференция **"Образование. Культура. Общество")**	26 февраля 2022 года
PSM 301	International Scientific Conference **"Psychology, Sports Science and Medicine**" (Международная научная конференция **"Психология. Спорт. Здравоохранение**")	27 февраля 2022 года
SITB 301	International Scientific Conference "**Security: Information, Technology, Behavior**". (Международная научная конференция **"Безопасность: Информация, Техника, Управление**")	28 февраля 2022 года
НИТП 326	Всероссийская (национальная) научно-практическая конференция **"Научные исследования в современном мире. Теория и практика"**	10 марта 2022 года
ФИПИ 326	Всероссийская (национальная) научная конференция **"Фундаментальные и прикладные исследования. Актуальные проблемы и достижения"**	11 марта 2022 года
СМИН 326	Всероссийская (национальная) научная конференция **"Современные методы и инновации в науке"**	12 марта 2022 года
ИПГС 326	Всероссийская (национальная) научно-практическая конференция **"Исследование и практика в социально-экономической и гуманитарной сфере"**	13 марта 2022 года
ВТ 196	Международная научная конференция "**Высокие технологии и инновации в науке"**	28 марта 2022 года
КО 196	Международная научно-методическая конференция **"Проблемы управления качеством образования"**	29 марта 2022 года
НБ 196	Всероссийская научно-практическая конференция **"Национальная безопасность России: актуальные аспекты"**	30 марта 2022 года
ПБ 196	Международная студенческая научная конференция **"Поколение будущего"**	31 марта 2022 года

Приглашаем к участию в конференциях научных и практических работников, преподавателей образовательных учреждений, докторантов, аспирантов, соискателей и студентов

Подробнее о конференциях Вы можете узнать на официальном сайте ГНИИ «Нацразвитие»:
WWW.NATSRAZVITIE.RU

Интересующие вопросы можно задать по телефону: **8 (812) 905-29-09**
или написать нам по адресу: **INFO@NATSRAZVITIE.RU**

НАУЧНЫЕ ЖУРНАЛЫ ГНИИ «НАЦРАЗВИТИЕ»

рецензируемые, печатные, DOI, elibrary.ru и др.

НАУЧНЫЙ ЖУРНАЛ «НАЦБЕЗОПАСНОСТЬ»

Общероссийский печатный научный журнал, публикующий результаты фундаментальных, поисковых и прикладных исследований, выполненных по различным наукам с позиций безопасности.

Все направления с позиций безопасности

ISSN 2782-3083 (6 раз в год)

Государственная регистрация в реестре СМИ: ПИ No ФС 77-80721

Публикация на русском и (или) английском языке

НАУЧНЫЙ ЖУРНАЛ «МЕТОД Z»

Общероссийский печатный научный журнал (фундаментальные, поисковые и прикладные исследования).

Технические, биологические, сельскохозяйственные науки

ISSN 2782-3091 (12 раз в год)

Государственная регистрация в реестре СМИ: ПИ No ФС 77-80686

Публикация на русском и (или) английском языке

НАУЧНЫЙ ЖУРНАЛ
«НАЦРАЗВИТИЕ. НАУКА И ОБРАЗОВАНИЕ»

Общероссийский печатный научный журнал (фундаментальные, поисковые и прикладные исследования).

Социально-экономические науки

ISSN 2782-3075 (12 раз в год)

Государственная регистрация в реестре СМИ: ПИ No ФС 77-80687

Публикация на русском и (или) английском языке

- Авторам бесплатно предоставляется журнал и свидетельство о публикации в электронном виде, благодарность научному руководителю.
- Всем статьям присваивается **индекс DOI.**

(DOI – международный цифровой идентификатор).

- Размещается в научной электронной библиотеке **elibrary.ru**
- Электронная версия (постатейно) размещается в электронной библиотеке: «**CIBERLENINKA**».
- **Все статьи индексируются** в **Google** Scholar.
- Печатный журнал рассылается по **ведущим библиотекам России.**

Основные финансовые условия:	**Руб.**
Публикация до 5 страниц (включительно) машинописного текста (без печатного сборника)	850
Каждая дополнительная страница (свыше 5 страниц)	210
Каждый печатный экземпляр журнала	400
Пересылка **за пределы РФ** дополнительно	750
Дополнительные финансовые условия:	**Руб.**
Справка о принятии материалов к публикации в электронной форме	150

WWW.NATSRAZVITIE.RU

INFO@NATSRAZVITIE.RU

ЗАРУБЕЖНЫЕ
МЕЖДУНАРОДНЫЕ НАУЧНЫЕ КОНФЕРЕНЦИИ
(ЛАТИНСКАЯ АМЕРИКА, ЕВРОПА, ВОСТОК)

совместно с издательством **Autofast Publisher** Managua, Nicaragua
на основе многолетнего сотрудничества с университетами
Востока, Европы и Латинской Америки

Название конференции	Страна
• Тенденции развития науки и глобальные вызовы	**НИКАРАГУА**
• Современные тренды мировой науки	**КИТАЙ**
• Современные наука и образование в контексте европейского опыта	**БОЛГАРИЯ, ФРАНЦИЯ**

- ✓ Конференции проводятся с возможностью стендового и заочного участия
- ✓ По итогам конференции издается сборник статей (в выходных данных указывается страна проведения, выходные данные на английском и испанском языках)
- ✓ Сборнику присваиваются международный стандартный книжный индекс **ISBN**
- ✓ Сборник регистрируется в **РИНЦ** и публикуется на сайте **Elibrary.ru**
- ✓ Сборнику и всем статьям присваивается индекс **DOI**

НАПРАВЛЕНИЯ КОНФЕРЕНЦИИ:

Секция 1	Архитектура	Секция 14	Педагогические науки
Секция 2	Астрономия	Секция 15	Политические науки
Секция 3	Биологические науки	Секция 16	Психологические науки
Секция 4	Ветеринарные науки	Секция 17	Сельскохозяйственные науки
Секция 5	Географические науки	Секция 18	Социологические науки
Секция 6	Геолого-минералогические науки	Секция 19	Технические науки
Секция 7	Журналистика	Секция 20	Фармацевтические науки
Секция 8	Искусствоведение	Секция 21	Физико-математические науки
Секция 9	Исторические науки	Секция 22	Филологические науки
Секция 10	Культурология	Секция 23	Философские науки
Секция 11	Литература	Секция 24	Химические науки
Секция 12	Медицинские науки	Секция 25	Экономические науки
Секция 13	Науки о Земле	Секция 26	Юридические науки

ФИНАНСОВЫЕ УСЛОВИЯ УЧАСТИЯ:

Публикация до 10 страниц для статьи на иностранном языке (английский, испанский)	3600 Руб.
Публикация до 10 страниц для статьи на русском языке	4800 Руб.
Каждый печатный экземпляр сборника	600 Руб.

КОНТАКТЫ:

Подробнее о конференциях**: http://natsrazvitie.ru/international_konferencii/**
Вопросы по участию в конференции: **8 (812) 905-29-09**
NATSRAZVITIE@GMAIL.COM