Интернет-журнал «Отходы и ресурсы» https://resources.today
Russian Journal of Resources, Conservation and Recycling

2022, №1 Том 9 / 2022, No 1, Vol 9 https://resources.today/issue-1-2022.html

URL статьи: https://resources.today/PDF/16ITOR122.pdf

DOI: 10.15862/16ITOR122 (https://doi.org/10.15862/16ITOR122)

Ссылка для цитирования этой статьи:
Рудзейт, О. Ю. Оценка уязвимостей протоколов передачи данных в информационных системах / О. Ю. Рудзейт, Ю. В. Добржинский, В. М. Титанов // Отходы и ресурсы. — 2022. — Т. 9. — № 1. — URL: https://mir-nauki.com/PDF/16ITOR122.pdf DOI: 10.15862/16ITOR122

For citation:
Rudzeyt O.U., Dobrzhinskii U.V., Titanov V.M. Vulnerability assessment of data transmission protocols in information systems. *Russian Journal of Resources, Conservation and Recycling*, 9(1): 16ITOR122. Available at: https://mir-nauki.com/PDF/16ITOR122.pdf. (In Russ., abstract in Eng.). DOI: 10.15862/16ITOR122

Рудзейт Олег Юрьевич
ФГАОУ ВО «Дальневосточный федеральный университет», Владивосток, Россия
Аспирант группы «Информатика и вычислительная техника», департамент информационной безопасности
E-mail: Rudzeyt18@mail.ru

Добржинский Юрий Вячеславович
ФГАОУ ВО «Дальневосточный федеральный университет», Владивосток, Россия
Старший преподаватель департамента информационной безопасности,
профессор департамента информационной безопасности
Кандидат технических наук
E-mail: dobrzhinskii.yv@dvfu.ru

Титанов Владислав Михайлович
ФГАОУ ВО «Национальный исследовательский университет ИТМО», Санкт-Петербург, Россия
Аспирант факультета «Программной инженерии и компьютерной техники»
E-mail: titanov.vm@mail.ru

Оценка уязвимостей протоколов передачи данных в информационных системах

Аннотация. В период бурной цифровизации общества современные технологии прочно укрепились во многих сферах экономики. Современные предприятия не ведут деловую активность без современных средств цифровых коммуникаций, которые позволяют обмениваться информацией как между объектами предприятия, так и осуществлять передачу данных пользователям за пределами внешнего периметра сети предприятия. Инфраструктура предприятия может иметь информационные уязвимости, которые злоумышленники используют с целью перехвата данных, атаки на системы предприятия, либо для атаки устройств пользователей системы. Такие атаки могут привести к сбоям в работе оборудования, отказам в обслуживании, программным ошибкам, потере данных и т. д. Согласно данным статистики компании Positive Technologies за 2021 год 33 % российских компаний были подвержены кибератакам с использованием уязвимости протоколов передачи данных компании, а 55 % крупных мировых компаний имеют серьезные уязвимости в периметре системы. В данной статье рассматриваются наиболее распространенные протоколы передачи данных, которые используются в автоматизированных системах управления технологическими процессами. Приводятся типы уязвимостей протоколов различных уровней модели OSI. Рассматриваются механизмы реализации уязвимостей и методы анализа сетевого трафика предприятия. Приводится статистика воздействий на протоколы передачи данных в различных

отраслях их использования, а также статистика по нарушениям регламентов информационной безопасности в компаниях. В основу статьи положена задача определения признаков воздействий и оценка защищенности протоколов с целью дальнейшей выработки решений для проведения мероприятий по противодействия воздействия на систему компаний.

Ключевые слова: система; уязвимость; протокол; данные; оценка; злоумышленник; сеть

Понятие уязвимостей информационных систем

Методы и исследования

Уязвимость информационной системы (ИС) — свойство информационной системы, обуславливающее возможность реализации угроз безопасности обрабатываемой в ней информации[1].

Угроза является событием или процессом, который, воздействуя с помощью специального ПО на компоненты ИС, может нанести урон компании.

Производя разведку, а в дальнейшем атаку, третье лицо использует уязвимости ИС. Поэтому одним из наиболее важных механизмов защиты данных предприятия является процесс поиска и устранения уязвимостей.

Угроза нарушения периметра защиты признается актуальной при наличии возможностей реализации данной угрозы с воздействием на слабые места системы корпорации.

Таким образом, качество и полнота выявления угроз зависят от полноты оценки возможностей нарушителя по эксплуатированию представленной угрозы и качественной оценке и анализа уязвимостей в системе защиты информации.

Угрозы проникновения в систему компании проявляются через взаимодействие со слабыми звеньями системы защиты. Угроза приводит к нарушению деятельности систем на конкретном объекте [1].

Основные уязвимости возникают по следующим причинам:

- ошибки архитектуры ПО или недочеты аппаратной составляющей;
- часть функционирующих процессов является неполноценной;
- слабая защищенность протоколов обмена информацией и интерфейса, уязвимости, допущенные при проектировании протокола передачи;
- ненадежная архитектура приложений и способов обмена информации между клиентом и сервером;
- сложные условия эксплуатации и расположения информации.

Классификация уязвимостей по источникам возникновения [2].

1. Уязвимости приложений драйверов аппаратных средств могут представлять:

- не декларированные возможности ПО, например, бэкдоров, скрытых схем авторизаций и функций программ;

[1] ГОСТ Р 50922-2006. Защита информации. Термины и определения [Текст]. — Введ. 2008-02-01. — М.: Изд-во стандартов, 2008.

- отсутствие необходимых и базовых средств защиты информации (СЗИ): установка логина и пароля при запуске приложения, хранение данных в легкодоступном месте и нешифрованном виде и др.;
- ошибки в приложениях, которые приводят к сбоям, зависаниям программы, ее принудительному закрытию.

Данный пункт имеет средний уровень вероятности реализации, т. к. производители прошивок и драйверов для экономии средств на разработке часто не устанавливают процедуры защиты в свой продукт и любой желающий может изменить его по своему усмотрению. Разработчики допускают ошибки во время создания программного обеспечения (ПО), которые выявляются через значительное количество времени не устраняются патчами. Чаще всего такие типы уязвимости встречаются в устройствах Интернета вещей, к которым можно получить физический доступ, скорректировать их конфигурацию, а администраторские пароль и логин невозможно изменить.

2. Уязвимости в процессе инициализации операционной системы (ОС) — перехват паролей или идентификаторов, модификация BIOS, перехват управления загрузкой с изменением конфигурации для несанкционированного доступа [3].

Данные уязвимости представляют низкий уровень вероятности, т. к. их эксплуатация требует высокий уровень подготовки, знаний об устройстве BIOS.

3. Уязвимости прикладного или специального ПО могут возникнуть:

- при несовместимости приложений, связанных с распределением ресурсов ИС;
- при изменении прикладных программных пакетов определенным образом. Данные изменения могут приводить к появлению новых уязвимостей или ошибок ПО;
- отсутствие необходимых и основных средств СЗИ.

Данный пункт имеет высокий уровень вероятности, т.к. не требуются углубленные знания языков программирования, многие прикладные программы имеют ошибки, которые не устраняются долгое время.

4. Уязвимости сетевого уровня модели OSI:

- аутентификация протокола ARP осуществляется передачей открытого текста в незашифрованном виде. Представленная уязвимость имеет среднюю вероятность реализации из-за того, что уязвимости на сетевом уровне широко известны, но могут быть не устранимы [4].

5. Уязвимости транспортного уровня модели OSI:

- отсутствие механизма предотвращения перегрузок буфера в протоколе UDP позволяет осуществить снижение производительности сервера, либо привести к отказу в обслуживании оборудования;
- в протоколе TCP не производится проверка правильности заполнения служебных заголовков пакета. Такая уязвимость может привести к снижению скорости обмена данными или полному разрыву соединений по протоколу.

Осуществление указанных уязвимостей имеют средний уровень вероятности. Для нарушения работы системы и ее производительности требуются специализированные знания.

6. Уязвимости сеансового уровня модели OSI:

- отсутствие поддержки аутентификации заголовков сообщений в протоколе SNMP может привести к превышению пропускной способности сети, либо к компрометации электронной почты и адресов отправителя;
- отправка паролей в протоколе FTP производится в открытом и нешифрованном виде. Также в случае передачи данных по протоколу FTP имеются несколько открытых портов, что предоставляет возможность получения удаленного доступа к устройствам;
- уязвимость системы доменных имен (DNS): отсутствие проверки аутентификации полученных данных от источника, которая может привести к фальсификации ответа DNS-сервера.

Данные уязвимости имеют средний уровень вероятности реализации, т. к. требуют высокий уровень подготовки и наличие специализированного ПО

7. Уязвимости прикладного уровня модели OSI:

В протоколе передачи Telnet заложен недостаток проектирования в виде передачи логина и пароля в открытом виде. Например, в протоколе передачи HTTP/HTTPS возможна компрометация куки из-за неправильной настройки передачи данных.

Для поиска уязвимых мест необходима разведка и подключение к самой СПД. Данные факты подключений могут быть распознаны различными путями. Наиболее распространенные способы — анализ сетевого трафика или изучение логов оборудования. Для анализа сетевого трафика и аудита безопасности чаще всего используются программы Nmap и PingInfoView которые присутствуют в дистрибутивах Linux: Kali Linux, Parrot OS. Кроме подключений внутри сети, что не исключает физического доступа к ресурсам компании, злоумышленник должен авторизоваться внутри домена, что позволит отследить и обнаружить следы вторжения. На рисунке 1 представлены подходы, которые использует хакер для доступа к сети информационной системы[2].

Современные специалисты в области проникновения в систему имеют большой выбор средств и методов для маскировки своего присутствия (рис. 2)[3]. Если специалист успешно произвел вторжение в систему, то наличие воздействия третьих лиц на протоколы возможно установить только с помощью анализ сетевого трафика. Для атаки из вне характерны определенные всплески нелегального трафика, использующего второстепенные каналы передачи данных, либо не часто используемые протоколы. Анализ пакетов производится с оценкой заголовков и служебных сигнатур (меток), передаваемых во время технологического обмена в сети.

Нарушитель в системе предприятия использует сетевое оборудование компании для перемещения внутри сети. Также вторжение резервирует часть общих сетевых ресурсов, доступ к которым предоставлен локальным администраторам. Для данных целей часто используется интерфейс удаленного вызова процедур (RPC). Для корректной работы интерфейса используется менеджер сервисов Service Control Manager (SCM) и сетевой ресурс IPCS (Inter-Process Communication) [5].

[2] Акутальные киберугрзоы II квартал 2020 года [Электронный ресурс] / Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q2/.

[3] The state of industrial cybersecurity in the era of digitalization // Kaspersky Industrial Cybersecurity Conference. 2020. [Электронный ресурс] URL: https://ics-cert.kaspersky.com/media/Kaspersky_ARC_ICS-2020 — Trend-Report.pdf (дата обращения: 01.03.2022).

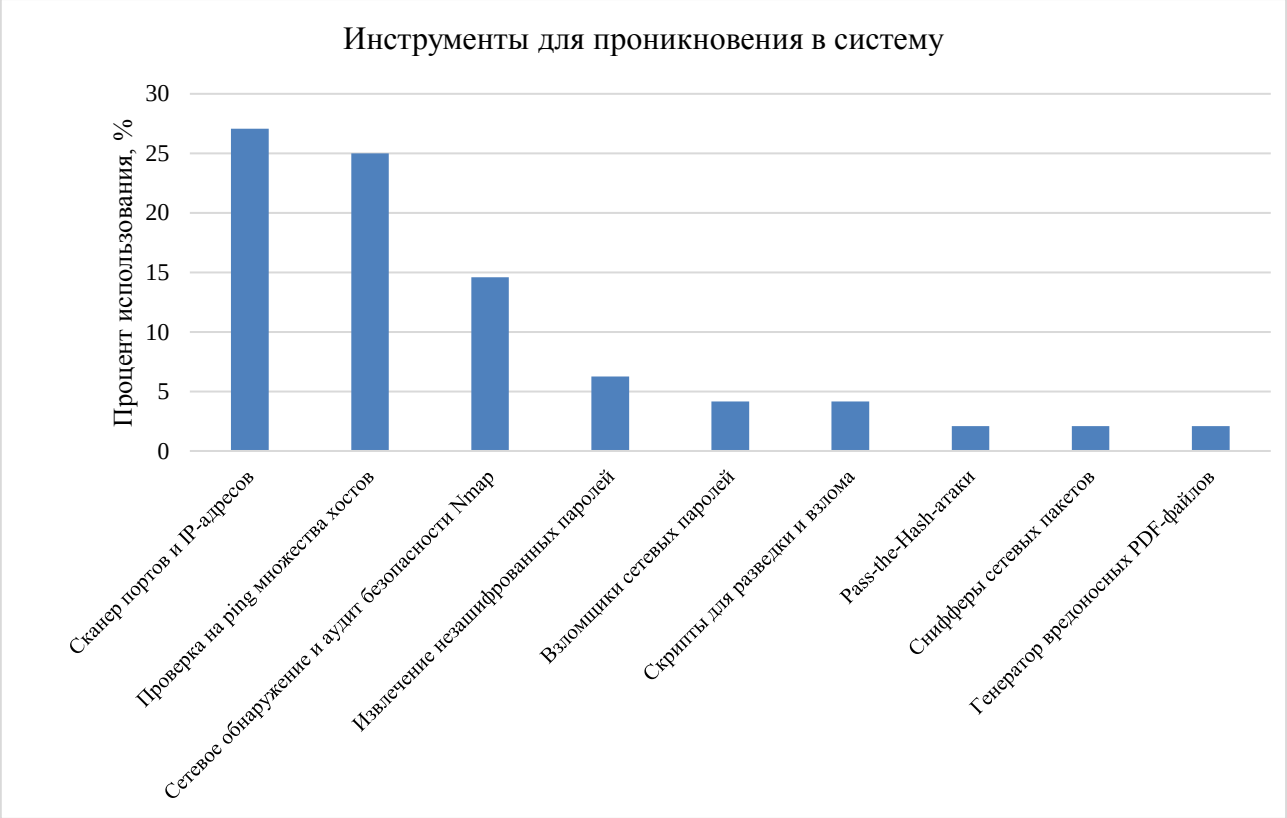

Рисунок 1. *Подходы, применяемые злоумышленниками для доступа в сеть*

Протокол RPC может работать поверх протокола SMB и поверх протокола TCP без использования протокола прикладного уровня модели OSI.

Помимо этого, для администрирования сетевых ресурсов и удаленного доступа к устройствам используется протокол Telnet, который является наиболее уязвимым, чем протоколы FTP, SFTP, SCP, SSH. Статистика, представленная лабораторией Касперского[4], показывает, что доля атак на протокол Telnet составляет 75,4 % против 11,59 % на SSH (рис. 3).

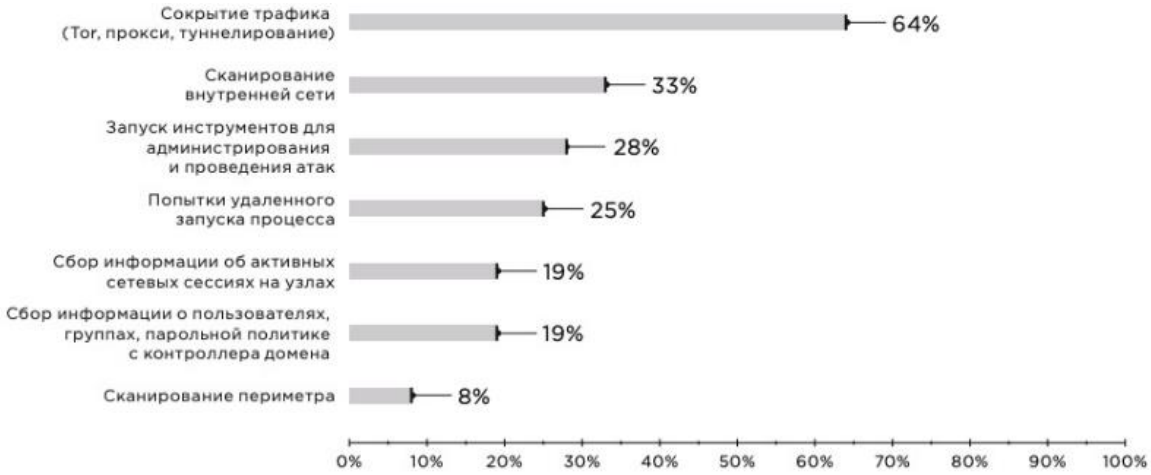

Рисунок 2. *События, выявляемые при эксплуатации уязвимостей сети*

[4] New trends in the world of IoT threats [Электронный ресурс] / Режим доступа: https://securelist.com/new-trends-in-the-world-of-iot-threats.

Чтобы выявить вторжение в систему, подключение к общим ресурсам и передачу нежелательной информации, потребуется сбор данных работы протокола SMB и извлечение информации из SMB-пакетов нелегального трафика [6].

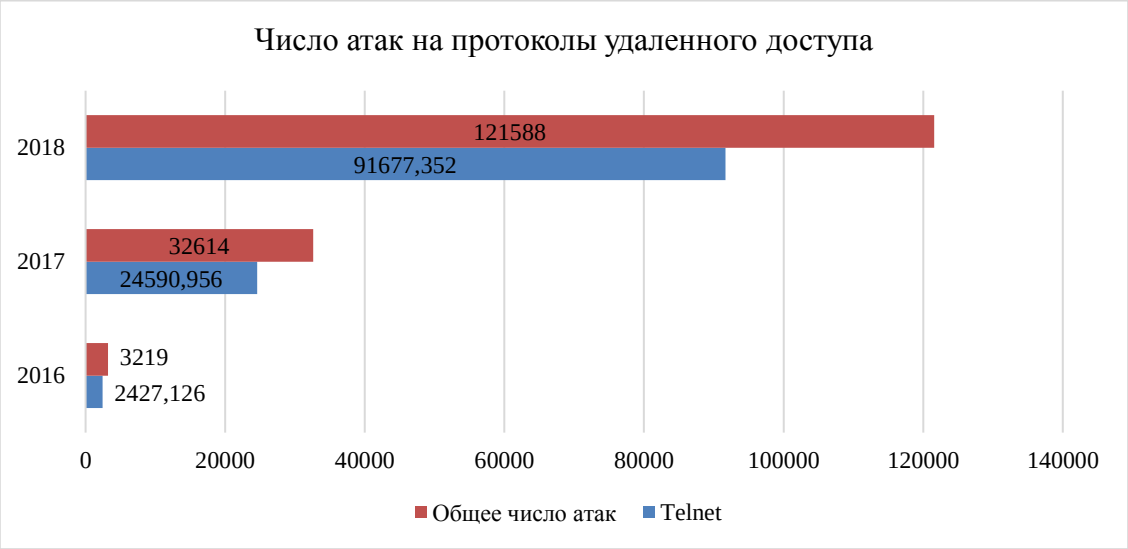

Рисунок 3. *Количество атак на протоколы удаленного доступа*

Злоумышленники подключаются к анонимной сети Tor, вводят в работу прокси-серверы и VPN-туннелирование для связи с серверами. Например, бэкдор ZxShell группировки APT41 устанавливает прокси-соединения по протоколам SOCKS и HTTP.

С помощью RPC реализуются и другие методы, например, account discovery. Отправка запросов сервису Security Accounts Manager по протоколу SAMR позволяет получить данные пользователей и групп в домене, а перебор идентификаторов SID с помощью сервиса Local Security Authority (LSARPC) предоставляет возможность узнать имена пользователей на удаленном узле.

Подобные технологии используются в деятельности администраторов, которые создают необходимость во внедрении способов автоматизации обнаружения RPC-вызовов и запросов к службам. Эффективным также является сигнатурный анализ, разрабатывающий точечные правила обнаружения меток, используемых для анализа сетевого трафика с учетом порядка команд и значений полей в заголовках пакетов.

Для проникновения внутрь периметра системы совсем необязательно знать пароль учетной записи сотрудника. Воздействие на основе процедуры «pass the hash» эксплуатирует уязвимости протокола NTLM, что позволяет подключаться к системе при помощи хеша пароля.

Если в системе присутствует аутентификация на основе Kerberos, то для выявления воздействий в виде перебора паролей потребуется анализ протокола Kerberos, который заключается в поиске сессий с ошибками [7].

Оценка уязвимости протоколов передачи данных

Для обмена данными или доступа сторонним ресурсам злоумышленники применяют протоколы прикладного уровня — HTTP, HTTPS, DNS, которые позволяют скрыть нелегитимный трафик (рис. 4).

В инфраструктуре 81 % компаний чувствительные данные передаются в открытом виде. Наряду с открытыми протоколами нередко выявляются нарушение в регламенте ИБ —

словарные пароли, хранение паролей в нешифрованном виде, установка приложений с удаленным доступом, отсутствие пароля для входа в систему и др.[5]

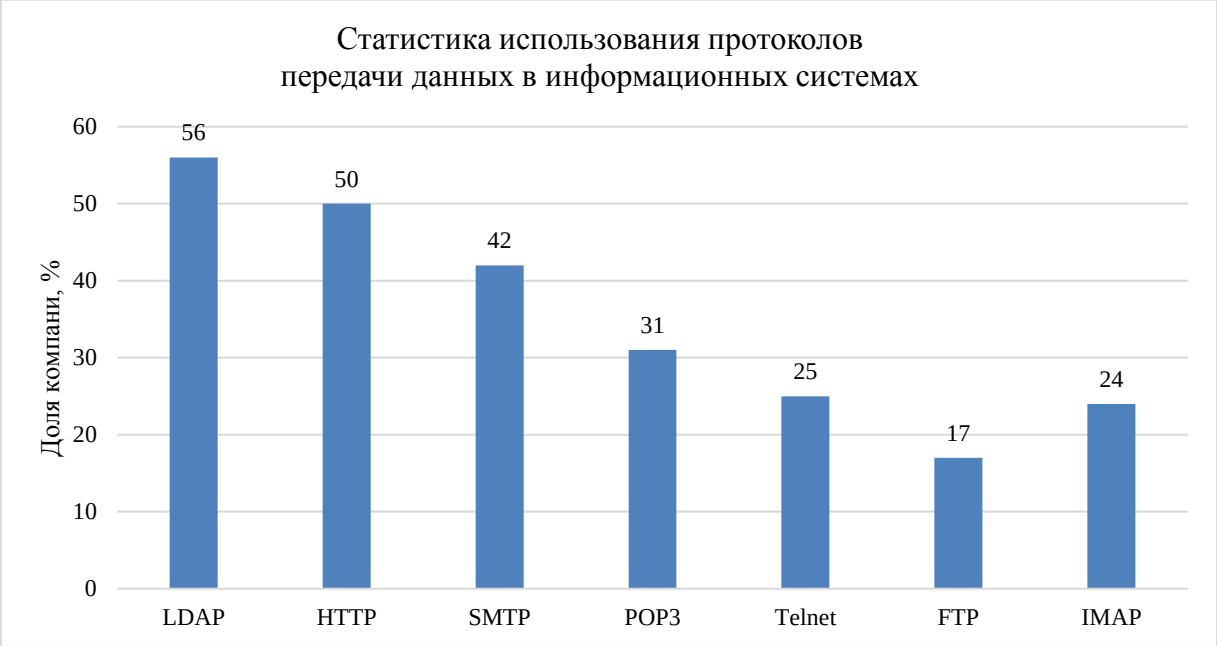

Рисунок 4. *Статистика использования незащищенных протоколов передачи данных в информационных системах*

В 56 % компаний выявлена передача данных по протоколу LDAP без шифрования, по которому работают службы каталогов. Администраторы используют их для централизованного администрирования и управления доступом к сетевым ресурсам.

Злоумышленники зачастую передают вредоносный код внутри туннеля, использующего протоколы: DNS, SMTP, ICMP [8]. На данный момент существуют следующие способы выявить признаки образования VPN-туннеля:

1. выявление признаков VPN-туннелирования с помощью отклонений в размере пакетов трафика;
2. определение сигнатур пакетов в трафике для создания туннеля.

В первом случае происходит определение признаков в сетевом трафике, сигнализирующих о наличии VPN-туннелирования. Для протокола DNS отклонением считаются большие размеры записей формата txt. Признаком ICMP-туннелирования является размер пакетов Echo Request и Echo Response.

Во втором случае происходит обнаружение определенных утилит. Например, эксплуатация инструментов ICMPTX и ICMPSH заметно по особым свойствам пакетов ICMP [9].

Для отражения атак на периметр информационной системы начальным этапом являются инструменты кластерного анализа трафика. В трафике идентифицируются определенные признаки, для выявления которых предварительно создают правила проверки трафика и специфические сигнатуры. Чтобы преодолеть первый этап защиты, атакующий использует методы обфускации, кодирования и шифрования. Существуют Base-подобные кодировки,

[5] Распространённые угрозы ИБ в корпоративных сетях [Электронный ресурс] / Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/network-traffic-analysis-2020/.

которые наиболее распространены в среде кибератак. При анализе трафика определяется содержание Base-подобной кодировки, затем применяются правила анализа к содержимому, которое предварительно декодируется.

Поведенческий анализ является одним из самых надежных способов борьбы с обфускацией. Данный способ требует консолидации алгоритмов анализа и проверки программного кода в безопасном виртуальном окружении.

Однако возникает проблема — распознавание воздействия на систему при шифровании трафика. Одним из подходов распознавания подозрительной активности в зашифрованном канале является расшифровывание и анализ содержимого в трафике с применением атаки «Men in the Middle». Применением нестандартных алгоритмов и SSL pinning вносят некоторые ограничения на применение анализа трафика активными методами.

Существуют и пассивные методы анализа. К ним относится поиск признаков нежелательной активности в зашифрованном трафике, которые могут быть идентифицированы через второстепенные или скрытые каналы, анализ длин пакетов и последовательности их перемещения [10].

В большинстве случаев Вредоносное ПО (ВПО) передает служебные данные, составляющие внутренний протокол или процедуру взаимодействия между клиентом и сервером. Данные об объекте, на который происходит воздействие, передаются только в зашифрованном виде. Во время шифрования передаются пакеты, имеющие определенную длину. На основе сформированной длины пакетов устанавливаются правила анализа длин пакетов ответов и запросов к системе.

Политики безопасности организаций запрещают сотрудникам посещать сомнительные ресурсы, скачивать торренты, устанавливать мессенджеры, использовать утилиты для удаленного доступа. Достаточно отметить, что нарушения регламентов информационной безопасности наблюдаются в 94 % компаний (рис. 5).

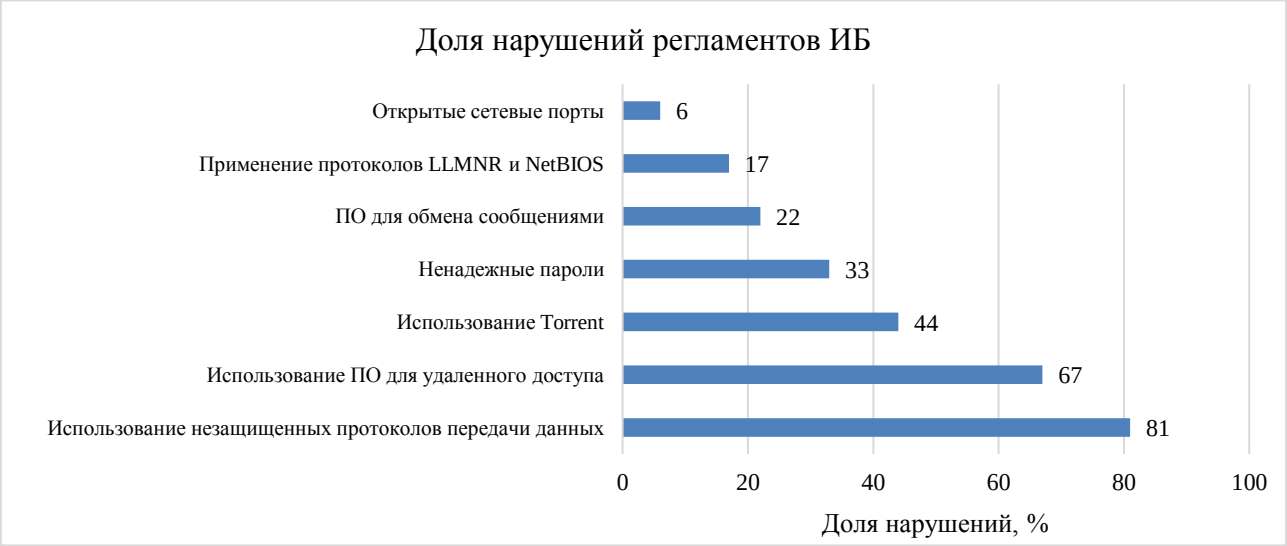

Рисунок 5. *Статистика нарушений регламентов ИБ в компаниях*

Заключение

Методы воздействия на протоколы передачи данных с целью эксплуатации уязвимостей постоянно совершенствуются и появляются новые образцы ВПО. Под конкретную СПД может создаваться целевой образец, позволяющий обойти традиционные средства идентификации. В

таком случае одиночная сигнатурная защита не эффективна и результативным средством становится анализ трафика.

Анализ сетевого трафика может служить дополнением к имеющимся средствам обнаружения нелегальной деятельности в системе. Системы оценки защищенности реализуют различные технологии, позволяющие совместить рассмотренные в статье подходы к построению защищенных СПД. Т. к. на данный момент все системы используют уже устаревающие протоколы передачи данных, в которых заложены уязвимости при их проектировании, то необходимо создать систему предварительной и рациональной оценки их защищенности. Также все представленные методы теряют свою эффективность с учетом антропогенных факторов, которые приводят к нарушения регламентов ИБ и увеличивает вероятность получения доступа в систему посторонним лицам. С внедрением новых технологий увеличивается количество передаваемой информации, что приводит к более легкому сокрытию нелегального трафика. Возрастание объема данных увеличивает нагрузку на систему предприятия, поэтому требуется разработка и внедрение новых подходов к оценке защищенности протоколов передачи данных. Наиболее перспективным направлением в данной области представляется использование систем искусственного интеллекта. Такие технологии позволяют автоматизировать оценку трафика и производить его мониторинг в режиме реального времени. Внедрение новых методов оценки защищенности может привести к новому этапу организации системы передачи внутри предприятия — использование сетей на основе намерений. Представленный в статье анализ позволяет утверждать, что без внедрения современных систем автоматизации, в первую очередь обучения и идентификации сигнатур признаков воздействий не решить задачу научного исследования.

ЛИТЕРАТУРА

1. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. — М.: ГЛТ, 2016. — 586 с.
2. Дементьев В.Е., Чулков А. А. Кибервоздействия на протоколы передачи данных // Известия ТулГУ. Технические науки. 2020. № 10. URL: https://cyberleninka.ru/article/n/kibervozdeystviya-na-protokoly-setey-peredachi-dannyh (дата обращения: 09.04.2022).
3. Боровиков А.Ю., Маслов О.А., Мордвинов С.А., Есафьев А.А. Способ создания доверенной аппаратно-программной платформы для применения в информационных системах специального назначения // Безопасность информационных технологий, 2021. Т. 28. № 4 С. 104–117. DOI: http://dx.doi.org/10.26583/bit.2021.4.08.
4. Alhaidary M. et al. Vulnerability analysis for the authentication protocols in trusted computing platforms and a proposed enhancement of the offpad protocol. IEEE Access. 2018. Vol. 6. P. 6071–6081. DOI: http://dx.doi.org/10.1109/ACCESS.2017.2789301.
5. Нестеров С.А. Основы информационной безопасности / С.А. Нестеров. — М.: Лань, 2016. — 324 с.
6. Cremers C.J.F., Lafourcade P. Comparing State Spaces in Automatic Security Protocol Verification. ETH Technical Report. 2007. No. 558. 26 p.
7. Козлов А.В. Тестирование и анализ атак на криптопротокол Kerberos с помощью программного стенда системы аутентификации // журнал «Информатика и вычислительная техника и управление», 2021 № 5. DOI: 10.37882/2223-2966.2021.05.16.
8. Соколов, А.В. Защита информации в распределенных корпоративных сетях и системах / А.В. Соколов, В.Ф. Шаньгин. — М.: ДМК Пресс, 2016. — 656 с.
9. K. Stokes, B. Yuan, D. Johnson, and P. Lutz, ICMP Covert Channel Resiliency. Dordrecht: Springer Netherlands, 2010, pp. 503–506.
10. Дементьев В.Е. Методика оценки комплексного информационного воздействия на протоколы обработки данных информационно-телекоммуникационной сети // Вопросы безопасности. 2016. № 4. С. 54–62.

Rudzeyt Oleg Urievich
Far Eastern Federal University, Vladivostok, Russia
E-mail: Rudzeyt18@mail.ru

Dobrzhinskii Uriy Vyacheslavovich
Far Eastern Federal University, Vladivostok, Russia
E-mail: dobrzhinskii.yv@dvfu.ru

Titanov Vladislav Mikhailovich
ITMO University, Saint-Petersburg, Russia
E-mail: titanov.vm@mail.ru

Vulnerability assessment of data transmission protocols in information systems

Abstract. During the period of rapid digitalization of society, modern technologies have become firmly established in many areas of the economy. Modern enterprises do not conduct business activity without modern means of digital communications, which allow the exchange of information both between the objects of the enterprise and the transmission of data to users outside the external perimeter of the enterprise network. The enterprise infrastructure may have information vulnerabilities that attackers use to intercept data, attack enterprise systems, or to attack the devices of system users. Such attacks can lead to hardware failures, service failures, software errors, data loss, etc. According to statistics from Positive Technologies in 2021, 33 % of Russian companies were exposed to cyberattacks using the vulnerability of the company's data transmission protocols, and 55 % of major global companies have serious vulnerabilities in the perimeter of the system. This article discusses the most common data transmission protocols that are used in automated process control systems. Types of vulnerabilities of protocols of various levels of the OSI model are given. The mechanisms of vulnerability implementation and methods of analyzing enterprise network traffic are considered. The statistics of impacts on data transmission protocols in various industries of their use, as well as statistics on violations of information security regulations in companies are provided. The article is based on the task of determining the signs of impacts and assessing the security of protocols in order to further develop solutions for measures to counteract the impact on the system of companies.

Keywords: system; vulnerability; protocol; data; evaluation; attacker; network