DOI: 10.25728/avtprom.2020.07.04

Обзор рекомендаций по безопасной удаленной работе для предприятий критической инфраструктуры и не только

Ю.С. Дащенко (Kaspersky ICS CERT)

Рассматриваются проблемы безопасности удаленной работы предприятия критической инфраструктуры. Проанализировано, насколько удаленный режим работы влияет на изменение ландшафта угроз. Приведено сравнение рекомендаций по безопасной удаленной работе в условиях COVID-19, опубликованных различными отечественными и зарубежными организациями.

Ключевые слова: безопасная удаленная работа, предприятия критической инфраструктуры, кибербезопасность.

Несмотря на пандемию COVID-19, большинство сотрудников, вовлеченных в технологические процессы предприятий критической инфраструктуры, по-прежнему работали в обычном (не удаленном) режиме. Это необходимо для обеспечения непрерывности функционирования предприятий. Однако административный персонал, напрямую не связанный с поддержанием технологических процессов, во многих случаях все же переведен на удаленную работу. Столь масштабное изменение породило многочисленные обсуждения проблемы безопасности удаленной работы среди профессионального сообщества информационной безопасности (ИБ), в том числе в сфере промышленной кибербезопасности.

Удаленный режим работы офисных сотрудников, а также повышение общего уровня тревожности персонала в условиях пандемии могут приводить к снижению бдительности работников предприятий в отношении угроз информационной безопасности. Например, вероятность того, что сотрудник, получив фишинговое письмо[1], использующее «горячую» тему COVID-19 [1], откроет вложение или кликнет по ссылке, повышается. Соответственно, растет и вероятность заражения его компьютера. Напомним, что многие инциденты информационной безопасности в промышленных сетях, которые привели к нарушению технологического процесса, начинались с заражения компьютеров в корпоративном сегменте сети предприятия. Уже в апреле 2020 г. были известны примеры атак на промышленный сектор с использованием фишинговых писем, связанных с COVID-19 [2].

Отдельно остановимся на рисках, связанных с удаленным администрированием систем промышленной автоматизации. Средства удаленного администрирования применялись в системах промышленной автоматизации и до пандемии. По данным Kaspersky Security Network, в первом полугодии 2018 г. они использовались на 32% компьютеров АСУ. В 2019 г., по данным системы Shodan, число доступных через Internet систем промышленной автоматизации выросло [3].

Вероятно, что в условиях пандемии такие средства будут использоваться чаще. Средства удаленного администрирования потенциально опасны для индустриальных сетей, и их использование требует повышенного внимания к обеспечению информационной безопасности. Это подтверждают результаты исследований различных реализаций системы удаленного доступа Virtual Network Computing (VNC), широко распространенной на объектах промышленной автоматизации.

В сложившейся ситуации предприятиям, особенно критической инфраструктуры, необходимо принять меры для минимизации возможных рисков. Поэтому регуляторы в сфере информационной безопасности, в том числе кибербезопасности критической инфраструктуры, подготовили рекомендации по безопасной удаленной работе.

Очевидно, что средства удаленного администрирования продолжат использовать на предприятиях критической инфраструктуры и в дальнейшем, поэтому рекомендации по безопасной удаленной работе будут актуальны и после окончания пандемии.

Основные рекомендации по организации безопасного удаленного доступа к системам промышленной автоматизации можно найти в следующих документах.

1. Рекомендации ICS-CERT по конфигурированию и управлению удаленным доступом к системам промышленной автоматизации ICS-CERT — Configuring and Managing Remote Access for Industrial Control Systems.

2. Стандарт безопасности промышленных систем управления NIST SP 800-82 Rev.2 «Guide to Industrial Control Systems (ICS) Security».

3. Рекомендации ENISA «Communication network dependencies for ICS/SCADA Systems».

Рекомендации, опубликованные в связи с пандемией

1. *ФСТЭК России* опубликовала рекомендации по обеспечению безопасности объектов КИИ при удаленной работе в связи с COVID-19 (https://fstec.ru/). В своем информационном сообщении регулятор говорит о недопустимости использования удаленного доступа для управления промышленным оборудованием АСУ, которые при категорировании были отнесены к значимым объектам критической информационной инфраструктуры. В других случаях удаленный доступ

[1] Фи́шинг — вид Internet-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путем проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей.

Таблица. Сравнение рекомендаций по безопасной удаленной работе в условиях COVID-19

Рекомендации	ФСТЭК	НКЦКИ	SANS	NIST	ENISA	CISA
Проведение инструктажа с персоналом о правилах безопасной удаленной работы	+	+	+	-	-	+
Определение перечня устройств, которые будут предоставлены работникам для удаленной работы. Запрет на использование личных устройств	+	-	-	+	-	-
Определение перечня ресурсов, к которым будет предоставляться удаленный доступ	+	-	-	+	-	-
Назначение минимально необходимых прав пользователям при удаленной работе	+	+	-	+	+	-
Идентификация удаленных устройств, предоставление доступа на основе «белых списков»	+	-	-	+	-	-
Исключение доступа посторонних лиц к удаленным рабочим местам	+	+	+	-	-	-
Выделение в отдельный домен устройств, используемых для удаленной работы сотрудников	+	-	-	+	-	-
Двухфакторная/многофакторная аутентификация работников	+	+	+	+	-	+
Организация защищенного удаленного доступа с использованием криптографии (VPN)	+	-	+	+	-	+
Применение средств антивирусной защиты информации с актуальными базами данных, их регулярное обновление	+	+	-	+	+	+
Запрет на установку ПО, за исключением необходимого, реализуемый средствами ОС или СрЗИ от НСД	+	-	-	-	-	-
Мониторинг безопасности систем, в том числе регистрация и анализ действий работников	+	+	-	-	-	+
Блокирование сеанса удаленного доступа при неактивности пользователя	+	+	-	-	-	-
Обеспечение возможности оперативного реагирования на инциденты	+	+	-	-	+	+
Сегментирование сети	-	+	-	+		-
Обновление всех сервисов и оборудования, которые используются для удаленного доступа (VPN, устройства сетевой инфраструктуры)	-	+	+	+	+	-
Контроль за подключением внешних устройств к устройствам, предназначенным для удаленного доступа	-	+	-	-	-	-
Ограничение скорости VPN соединений для приоритизации пользователей, которым потребуется более высокая пропускная способность	-	+	-	-	-	-
Запрет доступа в сеть с помощью сторонних сервисов, которые подключаются через промежуточные серверы и самостоятельно проводят авторизацию и аутентификацию	-	+	-	-	-	-
Использование терминального удаленного доступа в сеть к виртуальному рабочему месту со всеми установленными средствами защиты информации	-	+	-	-	-	-
Защита электронной почты двухфакторной авторизацией, проведение анализа электронной почты антивирусными средствами	-	+	-	-	-	-
Использование WPA2-шифрования при подключении к сети Internet с применением Wi-Fi	-	+	+	-	+	-
Управление паролями, использование сложных паролей	-	+	+	-	-	-
Шифрование информации на клиентских устройствах	-	-	-	+	-	-
Обеспечение возможности управления серверами удаленного доступа только с доверенных хостов авторизованными администраторами	-	-	-	+	-	-
Регулярное резервное копирование	-	-	-	-	+	-
Тестирование средств удаленного доступа с точки зрения производительности	-	-	-	-	-	+
Актуализация планов обеспечения непрерывности бизнеса	-	-	-	-	-	+

может быть использован с учетом предложенных рекомендаций.

Предложенные регулятором рекомендации включают технические и организационные меры, коррелирующие с положениями Приказа № 31 от 2014 г. Главным образом они направлены на контроль доступа к объектам (двухфакторная аутентификация, разграничение прав доступа и т. п.) и комплексную защиту задействованных каналов связи и конечных узлов сети (использование антивирусных решений, VPN, мониторинг безопасности).

В своем документе ФСТЭК России также ссылается на рекомендации другого российского регулятора — Национального координационного центра по компьютерным инцидентам.

2. *Национальный координационный центр по компьютерным инцидентам* (НКЦКИ) выпустил уведомление об угрозах безопасности информации, связанных с пандемией коронавируса (https://safe-surf.ru/specialists/news/645362/). Рекомендации НКЦКИ во многом схожи с рекомендациями ФСТЭК России и содержат ряд дополнительных технических мер, включая сегментирование сети и контроль за подключением внешних носителей, а также отдельные меры по противодействию угрозам, связанным с мошенничеством. И ФСТЭК России, и НЦКЦИ говорят о необходимости проведения инструктажа персонала по вопросам безопасной удаленной работы, в том числе информирования о фишинговых атаках, связанных с тематикой COVID-19.

3. *Институт SANS* в документе «Security Awareness Deployment Guide — Securely Working at Home» собрал список своих материалов, которые могут быть полезны для проведения обучения сотрудников по безопасной работе из дома (https://www.sans.org/). Все материалы сгруппированы в три основных блока, которые посвящены: социальной инженерии, аутентификации и управлению паролями, обновлению систем. Дополнительно приводятся материалы по использованию VPN и Wi-Fi, обнаружению и реагированию на инциденты.

4. *Национальный институт стандартов и технологий США (NIST)* выпустил бюллетень, содержащий рекомендации по безопасному удаленному доступу и удаленной работе (https://csrc.nist.gov). Этот документ опирается на положения документа NIST Special Publication (SP) 800-46 Revision 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security, который был опубликован в 2016 г. и является актуальным на сегодняшний день.

5. *Американское агентство кибербезопасности и безопасности инфраструктуры (CISA)* опубликовало документ, в котором рассмотрело вопросы обеспечения кибербезопасности организаций в рамках глобального процесса управления рисками, связанными с COVID-19 (https://assets.documentcloud.org). Среди прочего, CISA рекомендует актуализировать планы обеспечения непрерывности бизнеса и протестировать возможности решений удаленного доступа, в том числе с точки зрения повышения их производительности.

6. *Агентство Европейского союза по кибербезопасности (ENISA)* опубликовало советы по кибербезопасности при удаленной работе (https://www.enisa.europa.eu). В дополнение к мерам, которые были изложены в рассмотренных выше документах, ENISA напоминает о необходимости регулярного выполнения резервного копирования.

Сравнение рекомендаций по безопасной удаленной работе в условиях COVID-19, содержащихся в перечисленных документах, приведено в таблице.

Заключение

На основе анализа различных рекомендаций по обеспечению безопасности при удаленной работе можно сделать вывод о том, что частичный перевод сотрудников промышленных предприятий (как и любых других организаций) на удаленную работу не требует реализации каких-либо особенных мер защиты, принципиально отличающихся от того, что и так должно быть реализовано на предприятии. Однако временное изменение режима работы сотрудников требует проведения дополнительной проверки достаточности и эффективности принятых мер защиты

Особое внимание должно быть уделено защите каналов связи (включая обнаружение и предотвращение атак), контролю доступа и защите конечных устройств пользователей, которые будут использоваться для удаленной работы. При невозможности предоставить персоналу устройства с настроенными средствами защиты (средства антивирусной защиты, межсетевого экранирования и пр.) все необходимые средства должны быть предоставлены пользователям для самостоятельного развертывания на их личных компьютерах.

Также необходимо работать с персоналом: информировать о возможных угрозах и проводить дополнительные инструктажи по правилам удаленной работы.

Таким образом, комплекс принятых технических мер в совокупности с административными мерами и мерами по подготовке сотрудников позволят обеспечить необходимый уровень кибербезопасности предприятий для противодействия существующим угрозам, в том числе при более активном использовании удалённого доступа.

Список литературы

1. *Seals T.* In COVID-19 Scam Scramble, Cybercrooks Recycle Phishing Kits. April 2020. https://threatpost.com
2. *Mercer W., Rascagneres P. and Ventura V.* PoetRAT: Python RAT uses COVID-19 lures to target Azerbaijan public and private sectors. April 2020. https://blog.talosintelligence.com/
3. *Matherly. J.* Trends in Internet Exposure. March 2020. https://blog.shodan.io/trends-in-internet-exposure.

Дащенко Юлия Сергеевна *– старший аналитик по информационной безопасности, Kaspersky ICS CERT. Https://ics-cert.kaspersky.ru*