НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

Обобщенные рекомендации по минимизации возможных угроз информационной безопасности информационным ресурсам Российской Федерации

ALRT-20220329.1 | 29 марта 2022 г.

TLP: WHITE

Описание	Настоящий бюллетень содержит список рекомендаций, направленных на минимизацию возможных угроз информационной безопасности, и адресован широкому кругу российских компаний и организаций.
Рекомендации	1. Провести инвентаризационные мероприятия, в рамках которых обратить особое внимание на: 1.1. Пул внешних IP-адресов. 1.2. Домены и поддомены, используемые организацией. 1.3. Устройства, организующие дополнительные каналы управления (3G/4G LTE, WiFi и т.п.) программными, программно-аппаратными или аппаратными средствами (out-of-band management решения). 1.4. Информационные ресурсы, имеющие доступные из сети Интернет открытые порты и функционирующие на них службы (сервисы). 1.5. Определение владельцев и уполномоченных лиц организаций/подразделений, в интересах которых функционирует каждая служба, а также лиц, ответственных за их эксплуатацию. 1.6. Средства защиты информации, используемые для обеспечения безопасности информационных ресурсов организации, доступных из внешних сетей, в том числе из сети Интернет (например: межсетевые экраны, системы обнаружения вторжений, средства защиты электронной почты). 1.7. Протоколы, используемые для администрирования информационных ресурсов организации. 1.8. Учетные записи, применяемые для администрирования информационных ресурсов, функционирующих во внешнем периметре организации (поиск действующих сервисных учетных записей, учетных записей без паролей или имеющих пароли, настроенные «по умолчанию», нестойкие к атаке типа «перебор по словарю» или применяемые ранее для регистрации на сторонних сервисах, размещенных в сети Интернет). 1.9. Учетные записи, применяемые для удаленного подключения как своих работников, так и специалистов подрядных организаций, в том числе выполняющих задачи по технической поддержке, к

информационным ресурсам, функционирующим во внутренней информационно-телекоммуникационной сети.

2. Для информационных ресурсов, доступных из сети Интернет:

2.1. Обеспечить размещение технических средств, используемых для обеспечения функционирования информационных ресурсов, на территории Российской Федерации. При этом не использовать технологические площадки филиалов иностранных компаний.

2.2. Отключить неиспользуемые в работе сетевые службы (сервисы).

2.3. Ограничить использование небезопасных протоколов управления информационными ресурсами организации (например: TELNET, SNMPv1, v2, HTTP).

2.4. Ограничить (при возможности) взаимодействие с программным интерфейсом приложения (API).

2.5. Ограничить доступ к необходимым для работы службам (сервисам):

- запретить удаленный доступ к информационным ресурсам, функционирующим во внутренней информационно-телекоммуникационной сети организации, без использования технологии VPN;
- запретить удаленный доступ к информационным ресурсам, участвующим в управлении производственными и технологическими процессами, а также к информационным ресурсам, относящимся к «Интернету вещей» (IoT-устройства);
- в рамках сервисного обслуживания запретить удаленное администрирование информационных ресурсов организации с IP-адресов, принадлежащих иностранным операторам связи. В случае необходимости указанного администрирования настроить контроль за указанными подключениями;
- осуществлять блокировку подключений с IP-адресов узлов TOR и VPN-провайдеров.

2.6. Исключить (при возможности) применение систем видеоконференцсвязи иностранного производства (Zoom, Skype и аналогичных им), а также систем удаленного администрирования (RAdmin, Team Viewer и аналогичных им).

2.7. В случае необходимости использования публичных NTP-серверов обеспечить применение NTP-серверов, функционирующих на территории Российской Федерации (например: ntp.msk-ix.ru (194.190.168.1).

2.8. Организовать (при возможности) двухфакторную аутентификацию для доступа к публичным информационным ресурсам организации.

2.9. Отказаться от использования github, Pastebin и их аналогов.

2.10. Отказаться от использования иностранных облачных сервисов (Google Docs/Drive, Dropbox и аналогичных им).

2.11. Разработать перечень нежелательных Интернет-ресурсов и ограничить к ним доступ пользователей организации.

2.12. Организовать собственное хранилище (с поддержкой версионности) используемых продуктов с открытым исходным кодом.

2.13. Организовать проверку файлов используемых продуктов с открытым исходным кодом на предмет вредоносного воздействия перед добавлением в собственное хранилище.

2.14. Прорабатывать техническую возможность функционирования информационных ресурсов организации с использованием в TLS криптографических алгоритмов ГОСТ.

3. Для веб-приложений:

3.1. Использовать защищенные протоколы TLS v1.2 (и выше) при прохождении процедуры аутентификации пользователей в веб-приложении.

3.2. Запретить предоставлять в выводе сообщений об ошибках следующую информацию:

- данные о структуре файловой системы (информация о версии операционной системы, директориях с системными файлами и системным программным обеспечением, включая пути к директориям и файлам);
- фрагменты программного или конфигурационного кода;
- сообщения об ошибках при передаче запросов в СУБД;
- SQL-выражения, используемые при доступе к базе данных.

3.3. Выдавать пользователю страницу-заглушку с кодом HTTP-ответа веб-сервера «200» при обработке ошибок веб-сервером.

3.4. По возможности ограничить использование при обработке веб-сервером данных в формате XML внешних сущностей (External Entity), внешних параметров сущностей (External Parameter Entity) и внешних описаний типа документа (External Doctype), а также JSON.

3.5. Запретить кеширование веб-форм ввода конфиденциальной информации. Выставить атрибут HTTPOnly у параметров cookie, значения которых не должны быть доступны сценариям,

выполняемым браузером. У параметров cookie, содержащих чувствительную информацию, необходимо выставить атрибут secure.

3.6. Проводить проверку корректности вводимых пользователем данных как на стороне клиента (с использованием сценариев, исполняемых браузером), так и на стороне сервера.

3.7. Использовать директивы в заголовках сообщений HTTP, определяющие применяемую кодировку. Исключить использование разных кодировок для разных источников входных данных.

3.8. Использовать параметризованные запросы (например, хранимые процедуры) для построения SQL-запросов. В случае отсутствия такой возможности, организовать процедуру предварительной обработки получаемых от пользователя данных (путем удаления метасимволов « ` – / *», а также следующих SQL-операторов: SELECT, UNION, ALTER, UPDATE, EXEC, DROP, DELETE и INSERT).

3.9. Осуществлять преобразование HTML-кода входного потока данных следующим образом:

- заменить < > на &lti >
- заменить () на &#40 и)
- заменить # на #
- заменить & на &#38.

3.10. Осуществлять фильтрацию входного потока данных (например, с использованием методов Server.HTMLEncode и HttpServerUtility.HTMLEncode в ASP и ASP.NET).

3.11. Запретить пользователю ввод данных, в которых допустимы HTML-теги <IMG> или <TABLE>.

3.12. Для подсистем управления сессиями пользователей:

- организовать авторизованному пользователю веб-приложения возможность самостоятельного завершения сеанса работы в веб-приложении.
- обеспечить гарантированное удаление идентификатора соответствующей сессии по завершении сеанса работы клиента веб-приложения.
- ограничить время жизненного цикла сессии пользователя.

3.13. Для подсистем разграничения доступа:

- организовать доступ к защищенным ресурсам веб-приложения только после прохождения процедуры аутентификации;
- обеспечить хранение аутентификационных данных пользователей веб-приложения только в криптографически защищенном виде;

- исключить хранение аутентификационных данных (от веб-приложений, СУБД, ТКО, FTP и т.п.) в файлах конфигурации, доступных путем обращения к ним по URL;
- исключить хранение в HTML-страницах аутентификационных данных, а также информации, позволяющей сделать вывод о структуре каталогов веб-приложения на веб-сервере;
- в случае, если в веб-приложении предусматривается возможность внесения изменений пользователем в принадлежащий ему профиль, внесенные изменения необходимо подтверждать дополнительной процедурой аутентификации;
- запретить использование заголовка REFERER в качестве основного механизма авторизации.

3.14. Отказаться от использования на веб-ресурсах (в том числе веб-сайтах) компонентов и контента, подгружаемых с внешних ресурсов, не контролируемых организацией.

3.15. В случае невозможности отказа от использования указанных компонентов и контента осуществлять их проверку на предмет вредоносного воздействия на отображаемую в браузерах пользователя информацию, а также возможность кражи аутентификационных данных и файлов-cookie пользователей. Далее осуществлять периодическую проверку их хэш-сумм. В случае изменения хэш-сумм – блокировать использование указанных компонентов и контента на веб-ресурсе и осуществлять их повторную проверку функциональности. В случае отсутствия потенциально вредоносного функционала – проводить дальнейшее сравнение по новой хэш-сумме.

4. Для службы электронной почты

4.1. Исключить практику использования общедоступных зарубежных почтовых сервисов для обмена сообщениями электронной почты.

4.2. Настроить (при возможности) уведомления пользователей в тексте сообщения электронной почты при получении его от внешнего отправителя.

4.3. Запретить неавторизованную отправку электронной почты с адресов почтового домена организации (any@«доменное имя организации»).

4.4. Запретить отправку сообщений на адреса электронной почты, не относящиеся к почтовому домену организации, от произвольных адресов электронной почты (any@any).

4.5. Использовать (при возможности) протокол передачи данных TLS v1.2 (и выше) для защиты почты, передаваемой между почтовым сервером организации и внешними почтовыми серверами.

4.6. Использовать протокол передачи данных TLS v1.2 (и выше) для защиты почты, передаваемой между пользователем и почтовым сервером организации (например: SMTPS, IMAPS или расширение STARTTLS).

4.7. Использовать технологии Sender Policy Framework (SPF, RFC 7208) и Domain Keys Identified Mail (DKIM, RFC 4871 и RFC 6376) для подтверждения легитимности сервера электронной почты организации.

4.8. Осуществлять контроль входящих сообщений электронной почты по критериям, предоставляемым технологиями SPF и DKIM.

4.9. Заблокировать (при возможности) получение в электронных письмах вложений с расширениями ADE, ADP, APK, APPX, APPXBUNDLE, BAT, CAB, CHM, CMD, COM, CPL, DLL, DMG, EX, EX_, EXE, HTA, INS, ISP, ISO, JAR, JS, JSE, LIB, LNK, MDE, MSC, MSI, MSIX, MSIXBUNDLE, MSP, MST, NSH, PIF, PS1, SCR, SCT, SHB, SYS, VB, VBE, VBS, VHD, VXD, WSC, WSF, WSH (список не исчерпывающий и может дополняться владельцами информационных ресурсов самостоятельно).

4.10. Настроить антивирусную проверку всех входящих сообщений электронной почты. Запретить открытие пользователями вложенных файлов в сообщениях электронной почты до их проверки антивирусными средствами и проверки (по возможности) их функционала в изолированной программной среде (типа «Песочница»).

5. Для службы DNS

5.1. Обеспечить наличие у организации прав на свои доменные имена.

5.2. Обеспечить разнесение ролей DNS-серверов «User Primary DNS Server» и «Domain Primary DNS Server» на разные физические и/или виртуальные серверы.

5.3. В части «Domain Primary DNS Server»:

- запретить рекурсивные запросы разрешения доменных имён;
- запретить разрешение доменных имён объектов, не относящихся к информационным ресурсам организации;
- настроить механизмы защиты от спуфинг-атак;
- запретить уведомления и перенос зон произвольными объектами сети Интернет. Настроить список доверенных DNS-серверов;
- настроить правила предварительной фильтрации поступающих запросов (Таблица № 1).

Таблица № 1: Правила фильтрации запросов.

Описание	IP-адрес источника	Сетевой порт источника	IP-адрес назначения	Сетевой порт назначения
Входящий запрос	Любой	53/udp; 53/tcp; >1023/udp; >1023/tcp.	IP-адрес DNS-сервера	53/udp; 53/tcp.
Ответ на запрос	IP-адрес DNS-сервера	53/udp; 53/tcp.	Любой	53/udp; 53/tcp; >1023/udp; >1023/tcp.

5.4. Запретить в качестве «User Primary DNS Server» использовать DNS-серверы, расположенные за пределами Российской Федерации (например, перейти на использование НСДИ).

6. Для парольной защиты

6.1. Использовать для формирования паролей последовательности длиной не менее 12 символов для пользователей и не менее 14 символов для администраторов и алфавит, состоящий как минимум, из строчных и прописных символов латинского алфавита и цифр (мощность алфавита составляет не менее 62 символов) и спецсимволов.

6.2. Пароль не должен содержать имя, фамилию, дату рождения, месяц, логин, название компании в любых словоформах. По возможности генерацию паролей осуществлять на основе псевдослучайных функций.

6.3. Настроить механизмы защиты от подбора аутентификационных данных. Использовать меры по временной блокировке учетных записей. Осуществлять мониторинг блокировок учетных записей на предмет попыток массовых аутентификаций.

6.4. Хранить аутентификационные данные только в криптографически защищенном виде.

6.5. Не применять одинаковые пароли для различных учетных записей.

6.6. Исключить практику хранения паролей пользователей в атрибутах их учетных записей.

6.7. Настроить срок действия пароля пользователей (рекомендуемое значение политики – не более 90 дней).

6.8. Удалить (заблокировать) неиспользуемые учетные записи (например: уволенных работников, работников подрядных организаций, срок договора на услуги которых истек).

6.9. Ограничить список учетных записей, обладающих правами администратора.

6.10. Организовать смену аутентификационных данных учетных записей пользователей, имеющих пароли, настроенные «по умолчанию» (в том числе от сервисных учетных записей), нестойкие к атаке типа «перебор по словарю» и (или) применяемые ранее для регистрации на сторонних сервисах, размещенных в сети Интернет.

7. Для информационно-телекоммуникационной сети организации:

7.1. Запретить техническими средствами подключение к информационно-телекоммуникационной сети организации сетевых объектов, не входящих в ее состав, в том числе личных средств вычислительной техники (ноутбуки, персональные компьютеры, файловые хранилища, маршрутизаторы и другие подобные устройства) работников организации.

7.2. Разработать политику маршрутизации сетевого трафика в информационно-телекоммуникационной сети организации, в которой предусмотреть ограничение удаленного доступа к управляющим интерфейсам телекоммуникационного оборудования, серверам и рабочим станциям администраторов.

7.3. Исключить сопряжение информационно-телекоммуникационной сети организации с информационными ресурсами организации, участвующими в управлении производственными и технологическими процессами.

7.4. Использовать для удаленного администрирования как информационных ресурсов, подключенных к информационно-телекоммуникационной сети, так и телекоммуникационного оборудования только защищенные протоколы (например, ssh, https).

7.5. Организовать в информационно-телекоммуникационной сети организации демилитаризованную зону и обеспечить размещение в ней информационных ресурсов, доступных из сети Интернет. Ограничить доступ из демилитаризованной зоны к другим информационным ресурсам информационно-телекоммуникационной сети.

8. Для контроля информационной безопасности:

8.1. Проводить на постоянной основе анализ информационных ресурсов на предмет наличия критических уязвимостей.

8.2. Проводить корректировку настроек программного обеспечения и используемых средств защиты информации с целью минимизации возможности эксплуатации уязвимостей в случае их выявления.

8.3. Отключить автоматическую установку обновлений безопасности для всех продуктов. Очередное обновление может содержать уязвимость или недокументированную возможность, которую смогут использовать злоумышленники.

8.4. Организовать мониторинг событий информационной безопасности, позволяющий оперативно реагировать на компьютерные инциденты в случае их возникновения.

8.5. Организовать резервное копирование критической информации (базы данных, образы операционных систем ключевых работников организации, конфигурационные файлы серверного и телекоммуникационного оборудования) в обязательном порядке на файловые хранилища (отчуждаемые носители информации), изолированные от информационно-телекоммуникационной сети организации.

8.6. Проводить тестирование восстановления из резервных копий.

8.7. Запретить отправку событий безопасности во внешние иностранные сервисы (например: Cloud SIEM, Cloud EDR, SOC, MDR и аналогичные им).