УТВЕРЖДАЮ
Руководитель
Юго-Восточного управления
_____ Е.Ю.Балндина
18 сентября 2019 года

ПРАВИЛА
реагирования на компьютерные и вирусные атаки, направленные на информационные системы и ресурсы органов власти Самарской области

Настоящие Правила являются методическим документом, призванным предотвратить, минимизировать последствия деструктивных компьютерных и вирусных атак на информационные системы и ресурсы органов власти Самарской области.

Органы власти, учреждения, подведомственные органам власти, обслуживающие локальную вычислительную сеть (далее – ЛВС) органа власти, обязаны выполнять требования Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», нормативные правовые акты Российской Федерации, регулирующих отношения в области защиты информации.

Документ предназначен для пользователей (государственных, муниципальных служащих, сотрудников государственных учреждений) и системных администраторов ЛВС. Под системным администратором понимается работник, ответственный за поддержание технических средств ЛВС в рабочем состоянии конкретного органа власти.

В органах власти Самарской области, материально–техническое обеспечение деятельности которых осуществляет департамент управления делами Губернатора Самарской области и Правительства Самарской области в соответствии с постановлением Правительства Самарской области от 21.05.2009 № 234 (далее – ДУД), под системными администраторами понимаются специалисты участка по эксплуатации компьютерной сети ГУСО «Служба эксплуатации зданий и сооружений» (далее – ГУСО).

Настоящие Правила могут быть скорректированы (дополнены) в зависимости от специфических условий построения и функционирования ЛВС конкретного органа власти, государственного учреждения.

1. Признаки и уровни критичности компьютерной и вирусной атаки

1.1. Низкий уровень критичности:

1.1.1. частые «зависания» и сбои в работе компьютера;

1.1.2. браузер «зависает» или ведет себя неожиданным образом (например, окно программы невозможно закрыть);

1.1.3. частое обращение к жесткому диску (часто мигает лампочка на системном блоке);

1.1.4. медленная работа компьютера при запуске программ;

1.2. Средний уровень критичности:

1.2.1. произвольно, без участия пользователя, на компьютере запускаются какие-либо программы;

1.2.2. неожиданно открывается и закрывается лоток CD-ROM устройства;

1.2.3. в почтовом ящике находится большое количество сообщений без обратного адреса и заголовка;

1.2.4. невозможно сохранять файлы в нужных каталогах;

1.2.5. ошибки при загрузке операционной системы;

1.3. Высокий уровень критичности:

1.3.1. невозможность загрузки операционной системы;

1.3.2. исчезновение файлов и каталогов или искажение их названий;

1.3.3. коллеги (знакомые) информируют пользователя о сообщениях от вас, которые вы не отправляли;

1.3.4. на экран выводятся предупреждения о попытке какой-либо из программ компьютера выйти в интернет, хотя пользователь никак не инициировал такое ее поведение;

1.3.5. на экран выводятся непредусмотренные сообщения, изображения и звуковые сигналы.

1.4. Определение уровней опасности компьютерной и вирусной атаки:

Количество заражённых (атакованных) устройств в течение 30 мин	С низким уровнем критичности	Со средним уровнем критичности	С высоким уровнем критичности
1 ПК	Низкий	Низкий	Низкий
2-3 ПК (1 кабинет)	Низкий	Низкий	Средний
2-3 ПК (разные кабинеты)	Средний	Средний	Высокий
4 и более ПК (1 кабинет)	Средний	Высокий	Высокий
4 и более ПК (разные кабинеты)	Высокий	Высокий	Высокий

2. Действия пользователя при обнаружении признаков компьютерной и вирусной атаки

2.1. В случае обнаружения не типичной работы компьютера (изменение стандартного режима работы программных средств, произвольный, без участия пользователя, запуск каких-либо программ, информационных окон, невозможность загрузки операционной системы или программ, оповещение антивируса и т.п.) информировать системного администратора, обслуживающего орган власти.

2.2. Отключить все внешние носители информации (до выяснения причин внешние носители информации не подключать к другим рабочим местам).

2.3. По указанию системного администратора отключить (при возможности) рабочее место от ЛВС, отключив кабель ЛВС от системного блока или выключить рабочее место.

2.4. До приведения рабочего места в работоспособное состояние руководствоваться указаниями системного администратора.

3. Действия системного администратора органа власти при обнаружении компьютерной и вирусной атаки

3.1. Определить уровень критичности вирусной атаки (пункт 1.1. – 1.3.).

3.2. Определить уровень опасности для информационной инфраструктуры органа власти (пункт 1.4.).

3.3. Реализовать комплекс оперативных мер по локализации инцидента:

№ п/п	**Низкий уровень опасности**	**Средний уровень опасности**	**Высокий уровень опасности**
	время реагирования не более 3 часов	время реагирования не более 1 часа	время реагирования не более 20 минут
1	Выключить сетевые устройства (сетевые порты), обеспечивающие функционирование зараженных хостов в сети, определить уровень или тип сетевого устройства.	Выключить сетевое устройство, обеспечивающее связь пользовательского и серверного сегментов сети, определить конкретное устройство, его месторасположение.	Выключить основное маршрутизирующее оборудование, обеспечивающее связь органа власти с КСПД Правительства Самарской области, определить конкретное устройство, его месторасположение.
2		Выключить сетевые устройства (сетевые порты), обеспечивающие функционирование зараженного сегмента сети, определить уровень или тип сетевого устройства.	Выключить сетевое устройство, обеспечивающее связь пользовательского и серверного сегментов сети, определить конкретное устройство, его месторасположение.
3			Выключить сетевые устройства (сетевые порты), обеспечивающие функционирование зараженного сегмента сети,

			определить уровень или тип сетевого устройства.

3.4. Проинформировать об инциденте руководство органа власти.

3.5. Проинформировать об инциденте:

- ДУД по телефону 221 – 41-16 (при обслуживании органа власти ГУСО),

- Центр обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные системы и ресурсы Самарской области (далее – Центр) по телефону: 8 (846) 2000125 (доб. 299) или по электронной почте: isc@rcu.samregion.ru.

3.6. Собрать все возможные сведения для последующего анализа и расследования причин инцидента.

3.7. Принять меры по ликвидации последствий инцидента совместно с причастными службами.

3.8. Оповестить пользователей органа власти о возможной угрозе компьютерной и вирусной атаки и характерных ее признаках (при наличии возможности по АИС ДД, громкой связи, иным способом).

3.9. Организовать дальнейший мониторинг информационной инфраструктуры органа власти имеющимися техническими средствами.

3.10. Составить и доложить руководству справку (докладную записку) с подробным описанием случившегося, принятых мерах, предложениях.

4. Превентивные меры по противодействию компьютерной и вирусной атаки и защите периметра локальной вычислительной сети

Превентивные меры органами власти проводятся постоянно.

Сотрудники органов власти Самарской области должны быть ознакомлены со «Сводом правил по безопасной работе сотрудников органов исполнительной власти Самарской области, государственных органов Самарской области, органов местного самоуправления муниципальных образований в Самарской области и подведомственных им организаций при использовании сети Интернет, осуществлении информационного

взаимодействия с сервисами государственных информационных систем» и настоящими Правилами.

Основными каналами заражения вирусными и шпионскими программами следует считать электронную почту (зараженные прикрепленные файлы) и подключаемые USB устройства (носители информации, радиомодемы, смартфоны).

Подключение ЛВС к сетям, выходящим за пределы контролируемой зоны, осуществляется только с использованием межсетевых экранов.

4.1. Установить политикой безопасности (например, средствами Kaspersky Security Center) запрет подключения к рабочим местам любых внешних устройств, не предназначенных для исполнения служебных обязанностей (сотовых телефонов, смартфонов, 3/4G модемов, посторонней периферии и т.п.).

4.2. Установить политикой безопасности (например, средствами Kaspersky Security Center) принудительный запуск процесса сканирования на вирусы внешнего USB-накопителя информации при его использовании на рабочей станции. Отмена процесса сканирования должна быть доступна только системному администратору.

4.3. Обеспечить настройку соответствующих политик средств антивирусного контроля на почтовом сервере органа власти (например, Kaspersky Anti-Spam).

4.4. Обеспечить своевременное обновление баз и версий антивирусного программного продукта (например, Kaspersky Endpoint Security 10 для Windows).

4.5. Контролировать использование пользователями сети Интернет в личных целях.

4.6. Обеспечить регулярное резервное копирование рабочей (служебной) информации, расположенной на серверах, на зарегистрированные внешние носители информации.

4.7. Обеспечить регулярное обновление операционной системы и прикладного программного обеспечения (после проверки совместимости с установленными программными продуктами).

4.8. Обеспечить регулярную антивирусную проверку серверного сегмента, подключение рабочих станций к серверам обновлений антивирусного программного продукта.

4.9. Обеспечить контроль неиспользуемых портов серверов и рабочих станций (в последнее время вредоносное программное обеспечение использует 139 и 445 TCP-порты);

4.10. Обеспечить настройку межсетевого экрана по включающему принципу (разрешен только трафик, соответствующий заданным правилам и запрещен весь остальной).

4.11. Осуществлять ремонт, модернизацию, переконфигурацию серверов, рабочих мест, установку дополнительного программного обеспечения уполномоченным лицом в присутствии системного администратора или системным администратором.

4.12. Осуществлять тщательное отслеживание входящей электронной почты Правительства Самарской области (.samregion.ru), обратив внимание на правильное написание адресов отправителя, прикрепленные файлы (они не должны быть исполняемыми, т.е. иметь расширения .com, .exe, .bat, .reg и другие)

Сотрудникам при использовании служебных рабочих мест запрещается:

- использовать доступ к сети Интернет в личных целях;

- посещать досугово-развлекательные сайты;

- передавать информацию ограниченного доступа через сеть Интернет (в том числе посредством электронной почты) без использования средств защиты информации;

- отключать установленное на рабочем месте антивирусное программное обеспечение;

- осуществлять массовые рассылки электронной почты неслужебного характера (спама);

- использовать для служебной деятельности иные сервисы электронной почты;

- скачивать и загружать исполняемые файлы с расширением .exe, .bat., .com, .reg, разрешать выполнение макросов в файлах документов с расширением .doc, .docx, .xls, .xlsx (если это заранее не оговорено);

- подключать к служебным компьютерам USB-устройства (посторонние носители информации, радиомодемы, смартфоны и пр.);

- использовать для служебной деятельности на рабочих местах иностранные Интернет-сервисы: систем обмена мгновенными сообщениями, голосовой и видеоинформацией (ICQ, QIP, Jabber, Viber, Whatsap, Skype и т.д.), облачных сервисов хранения информации (iCloud, Google Drive, Dropbox и т.п.), почтовых сервисов электронной почты (Gmail, Yahoo).