МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ ЗАБАЙКАЛЬСКОГО КРАЯ

ПРИКАЗ

г. Чита

2022 года №

О мониторинге инцидентов по киберугрозам

В соответствии с перечнем поручений Заместителя Председателя Правительства Российской Федерации Д.Н.Чернышенко от 6 марта 2022 года № ДЧ-П10-3408кс, с целью защиты информационной инфраструктуры образовательных организаций Забайкальского края, предупреждения и ликвидация последствий компьютерных атак на информационные ресурсы государственных информационных систем, обеспечения мер безопасности официальных сайтов образовательных организаций, организации работы по борьбе с киберугрозами, **п р и к а з ы в а ю:**

1. Создать рабочую группу по борьбе с киберугрозами в системе образования в следующем составе:

Шибанова Н.М., заместитель министра – начальник Управления общего образования и воспитания, руководитель группы;

Задираева Ю.А., ведущий менеджер (по мобилизационной работе);

Лхасаранов Б.Ц., заместитель министра;

Егоров Е.С., заместитель министра;

Швец И.Г., начальник Управления лицензирования, государственной аккредитации, надзора и контроля;

Мусина Е.А., начальник отдела контрольно-аналитической работы; ответственный по административно-организационным вопросам в области кибербезопасности в системе образования;

Никифорова Н.Ю., начальник отдела общего, специального образования;

Бойкова Н.М., заместитель начальника отдела профессионального образования, взаимодействия с учреждениями высшей школы и науки;

Никулин И.В., главный специалист-эксперт отдела контрольно-аналитической работы;

Казакова Л.И., проректор, директор Центра цифровой трансформации образования ГУ ДПО «Институт развития образования Забайкальского края», ответственный за решение технических вопросов, связанных с

кибербезопасностью региональных информационных систем и информационной инфраструктуры;

Раднаев Г.Ц., специалист по связям с общественностью, ответственный за мониторинг и анализ недостоверной и противоправной информации в сети «Интернет», в том числе в соцсетях (Контент-администратор);

Подборнов Д.А. - преподаватель - организатор ОБЖ ГПОУ «Читинский политехнический колледж», руководитель «Кибердружины»;

сотрудник Макрорегионального филиала «Сибирь» Бурятского филиала ПАО «Ростелеком» (по согласованию).

2. Рабочей группе (Шибанова Н.М.) обеспечить:

2.1. контроль подключения образовательных организаций к информационно-коммуникационной сети «Интернет» только посредством Единой сети передачи данных, постоянно;

2.2. мониторинг отключения обновления применяемого в информационных системах иностранного программного обеспечения и программно-аппаратных средств, страной происхождения которых является США и страны Европейского союза, а также исключение их автоматическое централизованное обновление посредством сети «Интернет», в срок до 15 апреля 2022 года;

2.3. план-график перехода образовательных организаций края на разрешенные информационные ресурсы российского производства, в срок до 25 апреля 2022 года;

2.4. использование видеоконференцсвязи региональной платформы и информационно-коммуникационной образовательной платформы СФЕРУМ для решения административно-организационных и учебных вопросов, постоянно;

2.5. контроль исключения использования встроенных видео- и аудио-файлов, интерфейсов взаимодействия API, «виджетов» и других ресурсов, загружаемых со сторонних сайтов, заменив их при необходимости гиперссылкой на такие ресурсы, постоянно;

2.6. проведение профилактических мероприятий, направленных на исследование существующих угроз и методов противоправных действий в области ИКТ, в срок до 01 апреля 2022 года, далее постоянно;

2.7. проведение организационно-методических занятий с работниками образовательных организаций по организации работы с киберугрозами в системе образования, в срок до 10 апреля 2022 года.

3. Рекомендовать руководителям органов местного самоуправления, осуществляющих управление в сфере образования, руководителям образовательных организаций обеспечить:

3.1.проведение аналогичных мероприятий на муниципальном уровне и уровне образовательной организации;

3.2. контроль выполнения мероприятий в соответствии с чек-листом для предотвращения киберугроз (приложение 1);

3.3. информацию по всем зафиксированным инцидентам кибератак направлять на f.cit@zabedu.ru.по форме приложения 2.

4. Начальнику отдела контрольно-аналитической работы (Мусина Е.А.) совместно с проректором, директором Центра цифровой трансформации образования ГУ ДПО «Институт развития образования Забайкальского края»

(Казакова Л.И.) сводную информацию по выявленным инцидентам направлять в Министерство просвещения Российской Федерации.

5. Контроль за исполнением приказа возложить на заместителя министра – начальника Управления общего образования и воспитания Шибанову Н.М.

И.о.министра Т.К.Клименко

СОГЛАСОВАНО:

Заместитель министра, начальник Управления
общего образования и воспитания Н.М.Шибанова

Начальник контрольно-аналитического отдела Е.А.Мусина

исп. Никифорова Н.Ю., 28 52 21

Приложение 1

Чек-лист
для предотвращения киберугроз

В образовательной организации организовать процесс управления уязвимостями и инцидентами информационной безопасности:

создать регламенты;

определить ответственных.

Использовать антивирусы, сетевые экраны и другие средства защиты информации, в том числе сервисы для защиты от DDoS-атак.

Проводить образовательные мероприятия, периодические проверки безопасности компьютеров сотрудников с целью предотвращения кибератак (например, социальная инженерия и фишинг).

Регулярно делать резервные копии важных систем и данных. Хранить копии отдельно от самих систем, чтобы избежать их шифрования программами-вымогателями.

Применять парольную политику:

не использовать одинаковые пароли для доступа к разным сервисам;

не использовать простые и скомпрометированные пароли;

пользоваться менеджерами паролей;

использовать двухфакторную аутентификацию везде, где это возможно.

В случае возникновения угрозы:

1. Анализ ситуации и оценка ущерба

Сначала нужно проанализировать ситуацию: является ли произошедшее действительно инцидентом ИБ и какой это тип инцидента. Далее важно оценить возможный ущерб и масштаб. Определить, какие компоненты инфраструктуры были затронуты. На этом этапе необходимо сохранить как можно больше данных об инциденте: логи систем и приложений, различные файлы и другие индикаторы компрометации.

Лучше всего сохранить резервные копии скомпрометированных систем. В дальнейшем это может понадобиться для расследования, а также в качестве доказательств в оперативных мероприятиях.

2. Локализация инцидента

Для минимизации дальнейшего ущерба необходимо локализовать инцидент, то есть например, заблокировать вредоносный трафик, изолировать зараженные системы от сети предприятия, отключить часть сервисов и функций, заблокировать скомпрометированные доступы.

3. Устранение уязвимостей

Нужно исправить уязвимости, которые привели к инциденту: установить обновления безопасности, удалить вредоносное ПО, сменить пароли и ключи доступа, которые могли быть скомпрометированы. Возможно, переустановить операционные системы.

4. Настройка средств защиты

Применить правила на сетевых экранах и выполнить необходимые настройки на других системах защиты информации. И, конечно, восстановить работоспособность затронутых систем.

5. Анализ причин и превентивные меры

На последнем этапе нужно проанализировать причины возникновения инцидента. При необходимости скорректировать процедуры реагирования на инциденты. И разработать меры для предотвращения подобных инцидентов в будущем.

Приложение 2

Информация об инциденте
о проведении кибератак

ГО/МОУО_____

1. Наименование образовательной организации_____
2. Суть инцидента_____
3. Источник угрозы (адрес сайта, адрес почты) _____
4. Принятые меры по блокированию угрозы_____
5. Приложения (скриншот, логи)
6. Ответственный_____