

Федеральное государственное казённое общеобразовательное учреждение
«Казанское суворовское военное училище
Министерства обороны Российской Федерации»

ПРИНЯТО

Протокол заседания
педагогического совета КСВУ
от «29» октября 2020 г. № 8

УТВЕРЖДАЮ

Начальник Казанского
суворовского военного училища

В. Миронченко
«29» октября 2020 г.



ПОЛОЖЕНИЕ
по разграничению доступа пользователей сети
интернет с учетом политики безопасности в ФГКОУ
«Казанское суворовское военное училище»

I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящие Положение по разграничению доступа пользователей сети интернет с учетом политики безопасности в федеральном государственном казённом общеобразовательном учреждении «Казанское суворовское военное училище Министерства обороны Российской Федерации» (далее - Положение) разработано в целях функционирования эшелонированной системы контроля доступа обучающихся к ресурсам сети Интернет.

2. Настоящее положение определяет организацию взаимодействия по вопросам эффективного функционирования Эшелонированной системы контроля доступа для выполнения задач по профилактике и противодействию терроризму и экстремистской идеологии, предупреждению негативных социальных процессов, борьбе с наркоманией, анализу морально-психологического состояния обучающихся и организации порядка наполнения и уточнения политики ограничения доступа к нежелательным ресурсам сети Интернет.

3. Настоящие Положение имеет статус локального нормативного акта образовательного учреждения и распространяются на постоянный и переменный состав.

4. В настоящем Положении используются следующие термины:

глобальная политика ограничения доступа к нежелательным ресурсам сети Интернет Эшелонированной системы контроля доступа (глобальная политика ограничения доступа) - совокупность принципов, правил, процедур и приемов, регламентирующих процессы доступа к ресурсам сети Интернет обучающихся всех образовательных организаций, оснащенных комплексами средств фильтрации Эшелонированной системы контроля доступа;

локальная политика ограничения доступа к нежелательным ресурсам сети Интернет Эшелонированной системы контроля доступа (локальная политика ограничения доступа) - совокупность принципов, правил, процедур и приемов, регламентирующих процессы доступа к ресурсам сети Интернет обучающихся образовательной организации, оснащенной комплексом средств фильтрации Эшелонированной системы контроля доступа. Локальная политика ограничения доступа дополняет глобальную политику ограничения доступа;

Единая система централизованного доступа Вооруженных Сил Российской Федерации к ресурсам сети Интернет (СИДИ) - ведомственный сегмент сети Интернет, предназначенный для предоставления должностным лицам воинских частей доступа к ресурсам сети Интернет;

защита информации - деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на нее;

комплекс средств управления Эшелонированной системы контроля доступа (комплекс средств управления) - программно-аппаратный комплекс, являющийся ядром Эшелонированной системы контроля доступа и выполняющий функции управления подключенными комплексами средств фильтрации и формирования глобальной политики ограничения доступа;

комплекс средств фильтрации Эшелонированной системы контроля доступа (комплекс средств фильтрации) - программно-аппаратный комплекс, являющийся составной частью Эшелонированной системы контроля доступа, размещенный в образовательной организации и предназначенный для реализации функции фильтрации доступа обучающихся образовательной организации к ресурсам сети Интернет в соответствии с глобальной и сформированной в образовательной организации локальной политикой ограничения доступа, а также защиты от компьютерных атак;

компьютерная атака - целенаправленное воздействие программными (программно-техническими) средствами на информационные системы, информационно-телекоммуникационные сети, сети связи и автоматизированные системы управления, осуществляемое в целях нарушения (прекращения) их функционирования и (или) нарушения безопасности обрабатываемой в них информации;

мероприятия по защите информации - совокупность действий, направленных на разработку и (или) практическое применение способов и средств защиты информации;

перечень категорий нежелательных ресурсов сети Интернет (перечень нежелательных категорий) - список групп ресурсов сети Интернет, подлежащих блокировке в образовательных организациях,

автоматически отнесенных средствами защиты информации к определенной тематике по алгоритмам, заданным производителем;

перечень нежелательных доменных имен - конкретные сайты, доменные имена и ссылки на ресурсы сети Интернет, не попавшие в нежелательные категории, но подлежащие блокировке в образовательных организациях;

пользователи Эшелонированной системы контроля доступа -

должностные лица, отвечающие за выполнение мероприятий по анализу статистических данных Эшелонированной системы контроля доступа.

5. Вопросы защиты от компьютерных атак в данном Положении не рассматриваются и осуществляются в соответствии с действующим законодательством Российской Федерации и нормативными документами Министерства обороны Российской Федерации.

II. ОПИСАНИЕ ЭШЕЛОНИРОВАННОЙ СИСТЕМЫ КОНТРОЛЯ ДОСТУПА

6. Эшелонированная система контроля доступа представляет собой совокупность программных и аппаратных средств, реализующих функционал контроля доступа к ресурсам сети Интернет обучающихся в образовательных организациях и обеспечивающих:

- блокировку доступа обучающихся образовательных организаций к ресурсам, входящим в перечни нежелательных категорий и нежелательных доменных имен;
- возможность проведения заинтересованными центральными органами военного управления и образовательными организациями анализа посещаемых ресурсов сети Интернет на предмет выявления отклонений в поведении обучающихся;
- повышение уровня защищенности информационно – теле – коммуникационной инфраструктуры Интернет-контура образовательных организаций от воздействия компьютерных атак.

7. Эшелонированная система контроля доступа состоит из комплекса средств управления, размещенного в г. Москве, и комплекса средств фильтрации, расположенного в ФГКОУ «Казанском суворовском военном училище Министерства обороны Российской Федерации» (далее – Училище).

8. Комплекс средств фильтрации предназначен для непосредственного разграничения доступа обучающихся образовательных организаций к ресурсам сети Интернет, сбора статистических данных о попытках посещения обучающимися образовательных организаций нежелательных ресурсов сети Интернет, управления локальной политикой ограничения доступа, а также для защиты от компьютерных атак.

9. На основании Положения издается Приказ начальника Училища «О функционировании Эшелонированной системы контроля доступа обучающихся к ресурсам сети Интернет».

III. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ ЗАИНТЕРЕСОВАННЫХ ОРГАНОВ ВОЕННОГО УПРАВЛЕНИЯ ПО ВОПРОСАМ ФОРМИРОВАНИЯ И ВНЕСЕНИЯ ИЗМЕНЕНИЙ В ПЕРЕЧНИ НЕЖЕЛАТЕЛЬНЫХ КАТЕГОРИЙ И НЕЖЕЛАТЕЛЬНЫХ ДОМЕННЫХ ИМЕН

10. В процессе взаимодействия заинтересованных центральных органов военного управления и Училища формируются перечень нежелательных категорий и нежелательных доменных имен. Перечень нежелательных доменных имен может наполняться в общем и оперативном порядке.

11. Сведения о должностных лицах, отвечающих за формирование предложений по внесению изменений в перечни нежелательных категорий и нежелательных доменных имен, направляются (уточняются) в Главное военно-политическое управление Вооруженных Сил Российской Федерации (далее - ГВПУ ВС РФ) и в Восьмое управление Генерального Штаба Вооруженных Сил Российской Федерации (далее - ГШ ВС РФ) за подписью начальника Училища.

12. Общий порядок взаимодействия заинтересованных центральных органов военного управления и Училища при формировании перечня нежелательных доменных имен («тонкая» настройка):

- Училище по результатам анализа попыток доступа обучаемых к нежелательным сайтам, а также в целях обеспечения образовательного процесса, направляют 2 раза в год (до 1 июня, до 1 ноября) предложения в ГВПУ ВС РФ в перечень нежелательных доменных имен

- ГВПУ ВС РФ проводит анализ полученных предложений и согласовывает перечень нежелательных доменных имен с заинтересованными центральными органами военного управления;

- согласованный перечень нежелательных доменных имен утверждается заместителем Министра обороны Российской Федерации — начальником Главного военно-политического управления Вооруженных Сил Российской Федерации (первым заместителем начальника Главного военно-политического управления Вооруженных Сил Российской Федерации) 2 раза в год (до 1 июля, до 1 декабря);

- ГВПУ ВС РФ направляет утвержденный перечень нежелательных доменных имен в адрес заинтересованных центральных органов военного управления;

- Восьмое управление (далее - ГШ ВС РФ) осуществляет настройку средств защиты информации комплекса средств управления в соответствии с утвержденным перечнем нежелательных доменных имен.

IV. РАЗГРАНИЧЕНИЕ ЗОН ОТВЕТСТВЕННОСТИ СУБЪЕКТОВ ВЗАИМОДЕЙСТВИЯ В ЧАСТИ ЭКСПЛУАТАЦИИ ЭШЕЛОНИРОВАННОЙ СИСТЕМЫ КОНТРОЛЯ ДОСТУПА

13. Училище:

- осуществляют администрирование комплексов средств фильтрации, находящиеся в зоне ответственности образовательной организации, в том числе формируют локальную политику ограничения доступа;
- обеспечивают функционирование комплексов средств фильтрации в непрерывном (постоянном) режиме;
- организуют подключение всех автоматизированных рабочих мест (информационных систем) образовательной организации, предназначенных для доступа к ресурсам сети Интернет, через комплекс средств фильтрации;
- обеспечивают своевременное направление в Восьмое управление ГШ ВС РФ уведомлений об изменении состава самостоятельного абонентского пункта сети Интернет образовательной организации в соответствии пунктом 37 Инструкции;
- направляют отчеты о попытках посещения обучаемыми нежелательных ресурсов, заблокированных комплексами средств фильтрации Эшелонированной системы контроля доступа, и принятых мерах при выявлении отклонений в поведении обучающихся в адрес ГВПУ ВС РФ и Восьмое управление ГШ ВС РФ раз в полгода, к 1 июня и 1 ноября;
- формируют и направляют в ГВПУ ВС РФ предложения в перечни нежелательных категорий и нежелательных доменных имен (при необходимости).

V. ИНСТРУКЦИЯ АДМИНИСТРАТОРА КОМПЛЕКСА СРЕДСТВ ФИЛЬТРАЦИИ

14. В целях выполнения глобальной политики ограничения доступа обучающихся к ресурсам сети Интернет и локальной политики ограничения доступа администратор комплекса средств фильтрации должен осуществлять администрирование комплекса средств фильтрации, он обязан:

- контролировать, что бы все автоматизированные рабочие места (информационные системы) училища, предназначенные для доступа к ресурсам сети Интернет были подключены через комплекс средств фильтрации,
- следить за тем, что бы функционирование комплексов средств фильтрации находилось в непрерывном (постоянном) режиме,
- обеспечивать разграничение доступа обучающихся и сотрудников к ресурсам сети Интернет,
- проводить анализа посещаемости ресурсов сети интернет обучающимися не реже одного раза в месяц с оформлением акта проверки, постоянно обновлять перечень нежелательный ресурсов сети Интернет,

- при необходимости вносить предложения о внесении изменений в локальный акт политики ограничения доступа,
- проводить анализ посещаемости ресурсов сети интернет обучающимися не реже одного раза в месяц с составлением акта проверки,
- направлять отчеты о попытках посещения обучающимися нежелательных ресурсов, заблокированных комплексами средств фильтрации Эшелонированной системы контроля доступа, и принятых мерах при выявлении отклонений в поведении обучающихся в адрес ГВПУ ВС РФ и Восьмое управление ГШ ВС РФ раз в полгода, к 1 июня и 1 ноября,
- при необходимости отправлять предложения в ГВПУ ВС РФ в перечень нежелательных категорий и нежелательных доменных имен,
- следить за настройкой ноутбуков обучающихся в части ограничения подключения от WI-FI сетей, возможностью ограничения подключения USB устройств, а также не зарегистрированных установленным порядком USB накопителей,
- блокировать нежелательные сайты согласно утвержденного перечня.
- пополнять перечень нежелательный ресурсов сети Интернет в локальной сети училища в папке общая для всех подразделений, безопасность.

VI. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

15. Положение рассматривается и принимается на педагогическом совете и утверждается приказом начальника Училища.

16. Настоящее Положение принимается на неопределенный срок и вступает в силу с момента его утверждения.


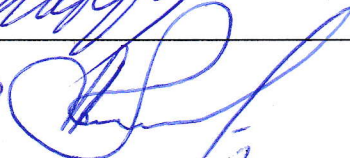
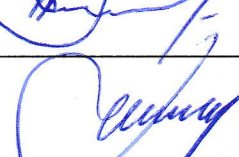


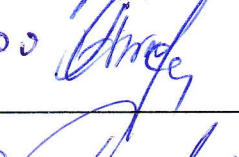
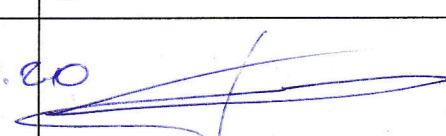
17. Положение может быть изменено и дополнено в соответствии с вновь изданными нормативными правовыми актами регионального, федерального органов управления образованием.

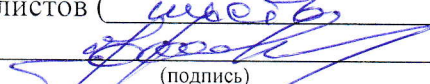
18. Изменения и дополнения к Положению принимаются на педагогическом совете в составе новой редакции Положения, которое утверждается начальником Училища. После принятия новой редакции Положения предыдущая редакция утрачивает силу.

19. Текст настоящего Положения подлежит размещению в установленном порядке на официальном сайте Училища.

ЛИСТ СОГЛАСОВАНИЯ

к Положению по разграничению доступа пользователей сети интернет с учетом политики безопасности в ФГКОУ «Казанское суворовское военное училище» на 6 страницах.

Должность сотрудника, осуществляющего визирование проекта локального акта	Дата визирования	Подпись руководителя (с расшифровкой)
Заместитель начальника училища (по учебной работе)	26.10.20	
Заместитель начальника училища (по инновационным образовательным технологиям)	26.10.2020	
Заместитель начальника училища (по воспитательной работе)	27.10.20	
Заместитель начальника училища (по тылу)	27.10.2020	
Начальник отделения кадров и строевого	28.10.2020	
Председатель профсоюзной организации училища	28.10.2020	
Юрисконсульт	26.10.20	

<p>В настоящем локальном акте пронумеровано, прошнуровано и скреплено печатью «Для пакетов. Казанское суворовское военное училище»</p> <p><u>6</u> листов (<u>шесть</u>)</p> <p> (подпись)</p>

Исп: Начальник лаборатории инновационных образовательных технологий
 Степанов А.М.
 тел.: вн. 51-33