



# УЧРЕЖДЕНИЯ ОБРАЗОВАНИЯ

Методическое пособие  
по информационной безопасности

 SMART-SOFT

Советы по  
IT-безопасности  
внутри





Фото: [www.kremlin.ru](http://www.kremlin.ru)

”

С помощью передовых телекоммуникаций мы откроем нашим гражданам все возможности цифрового мира. И это не только современные сервисы, онлайн-образование, телемедицина...

Люди смогут создавать в цифровом пространстве научные, волонтерские команды, проектные группы, компании. Для нашей огромной по территории страны такое объединение талантов, компетенций, идей — это колоссальный прорывной ресурс.

Президент РФ  
Владимир Путин

Источник: [www.kremlin.ru/events/president/news/56957](http://www.kremlin.ru/events/president/news/56957)



Фото: [www.kremlin.ru](http://www.kremlin.ru)

”

На сегодняшний день... не во всех школах интернет — скоростной. В рамках национального проекта «Образование» будет подключение именно к скоростному интернету.

Министр просвещения РФ  
Ольга Васильева

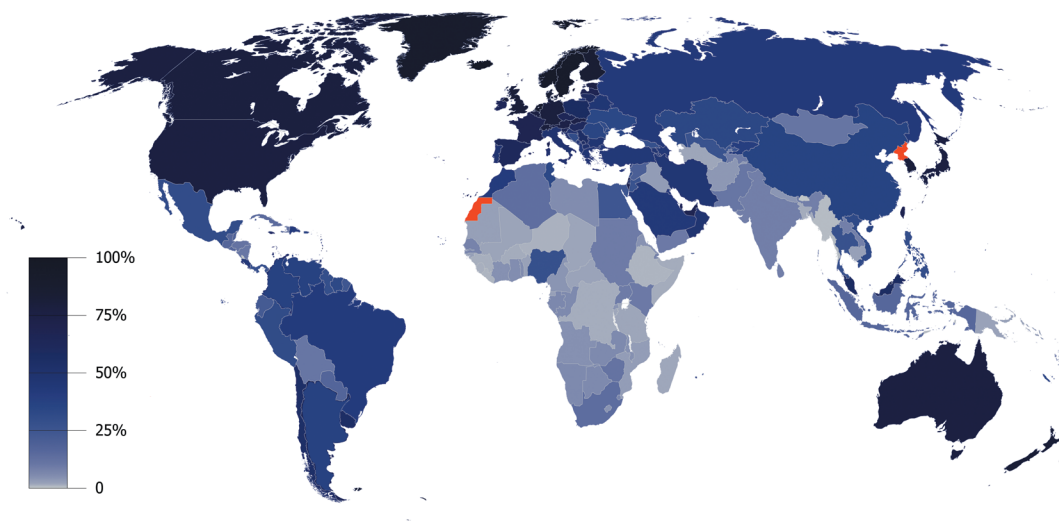
Источник: [www.ria.ru/20181230/1548933086.html](http://www.ria.ru/20181230/1548933086.html)

# Интернет и образование



Россия входит в список стран с высоким проникновением интернета (**более 75%** населения имеют доступ к Всемирной сети).

## КАРТА РАСПРОСТРАНЕНИЯ ПОЛЬЗОВАТЕЛЕЙ ИНТЕРНЕТА ПО ВСЕМУ МИРУ (% ОТ НАСЕЛЕНИЯ)



Источник: [www.ru.wikipedia.org/wiki/](http://www.ru.wikipedia.org/wiki/)

Интернет активно проникает в образование. Если в 2016 году (согласно проекту «Исследование российского рынка онлайн-образования и образовательных технологий») рынок онлайн-обучения в России составил 20,7 млрд рублей, то, по прогнозам, к 2021 году он вырастет более чем в 2,5 раза, до 53,3 млрд рублей.

2016 год

**1,8** трлн руб.

Весь рынок

**1,1% - 20,7** млрд руб.

Онлайн-образование



2021 год

**2** трлн руб.

Весь рынок

**2,6% - 53,3** млрд руб.

Онлайн-образование

## РЫНОК ОБРАЗОВАНИЯ В РОССИИ НА 2016 ГОД

|                        |                           |                           |                     |                           |                        |                    |
|------------------------|---------------------------|---------------------------|---------------------|---------------------------|------------------------|--------------------|
| Дошкольное образование | Общее среднее образование | Доп. школьное образование | Высшее образование  | Среднее проф. образование | Доп. проф. образование | Языковое обучение  |
| 462<br>млрд р.         | 572<br>млрд р.            | 130<br>млрд р.            | 386<br>млрд р.      | 146<br>млрд р.            | 105<br>млрд р.         | 31<br>млрд р.      |
| Онлайн-образование     | Онлайн-образование        | Онлайн-образование        | Онлайн-образование  | Онлайн-образование        | Онлайн-образование     | Онлайн-образование |
| 0,1%<br>0,6 млрд р.    | ~0%                       | 2,7%<br>3,6 млрд р.       | 1,8%<br>6,8 млрд р. | 0,4%<br>0,6 млрд р.       | 6,7%<br>7 млрд р.      | 7%<br>2,2 млрд р.  |

## ПРОГНОЗ НА 2021 ГОД

|                        |                           |                           |                    |                           |                        |                      |
|------------------------|---------------------------|---------------------------|--------------------|---------------------------|------------------------|----------------------|
| Дошкольное образование | Общее среднее образование | Доп. школьное образование | Высшее образование | Среднее проф. образование | Доп. проф. образование | Языковое обучение    |
| 548<br>млрд р.         | 699<br>млрд р.            | 149<br>млрд р.            | 336<br>млрд р.     | 175<br>млрд р.            | 103<br>млрд р.         | 31<br>млрд р.        |
| Онлайн-образование     | Онлайн-образование        | Онлайн-образование        | Онлайн-образование | Онлайн-образование        | Онлайн-образование     | Онлайн-образование   |
| 0,3%<br>1,7 млрд р.    | 1,5%<br>10 млрд р.        | 6,8%<br>10 млрд р.        | 4,4%<br>15 млрд р. | 1%<br>1,8 млрд р.         | 10,9%<br>11 млрд р.    | 10,7%<br>3,3 млрд р. |

Источник: [www.ewdn.com/files/russian\\_edtech\\_part1.pdf](http://www.ewdn.com/files/russian_edtech_part1.pdf)

К 2021 году:

- уменьшится количество обучающихся в сегменте высшего образования (в основном за счет постепенного упразднения программ специалитета);
- в соответствии с прогнозом, основанным на демографических данных Росстата, численность студентов, обучающихся по программам бакалавриата и специалитета, будет уменьшаться, а численность магистров — расти;
- все сегменты образования (включая дошкольное и общее среднее) будут включать дистанционное обучение.



Проникновение интернета в образование сопровождается ростом цифровых угроз.



# Цифровые угрозы в сфере образования





### ЗАПРЕЩЕННЫЕ РЕСУРСЫ

могут быть доступны учащимся на компьютерах учреждения.

В частности, интернет-ресурсы, пропагандирующие суицид и содержащие информацию, способную причинить вред здоровью и развитию детей.



### ВРЕДНЫЙ КОНТЕНТ

может находиться на страницах формально разрешенных ресурсов (блоги, форумы, сайты).



### НЕЦЕЛЕВОЕ ИСПОЛЬЗОВАНИЕ ИНТЕРНЕТА

может отвлекать от процесса обучения (социальные сети, мессенджеры, видеохостинги, игровые порталы, онлайн-казино, сайты знакомств и т. п.)



### ВЗЛОМ СЕТИ ОРГАНИЗАЦИИ ЧЕРЕЗ ИНТЕРНЕТ-КАНАЛЫ

может дать в руки хакерам персональную информацию и другие конфиденциальные данные.

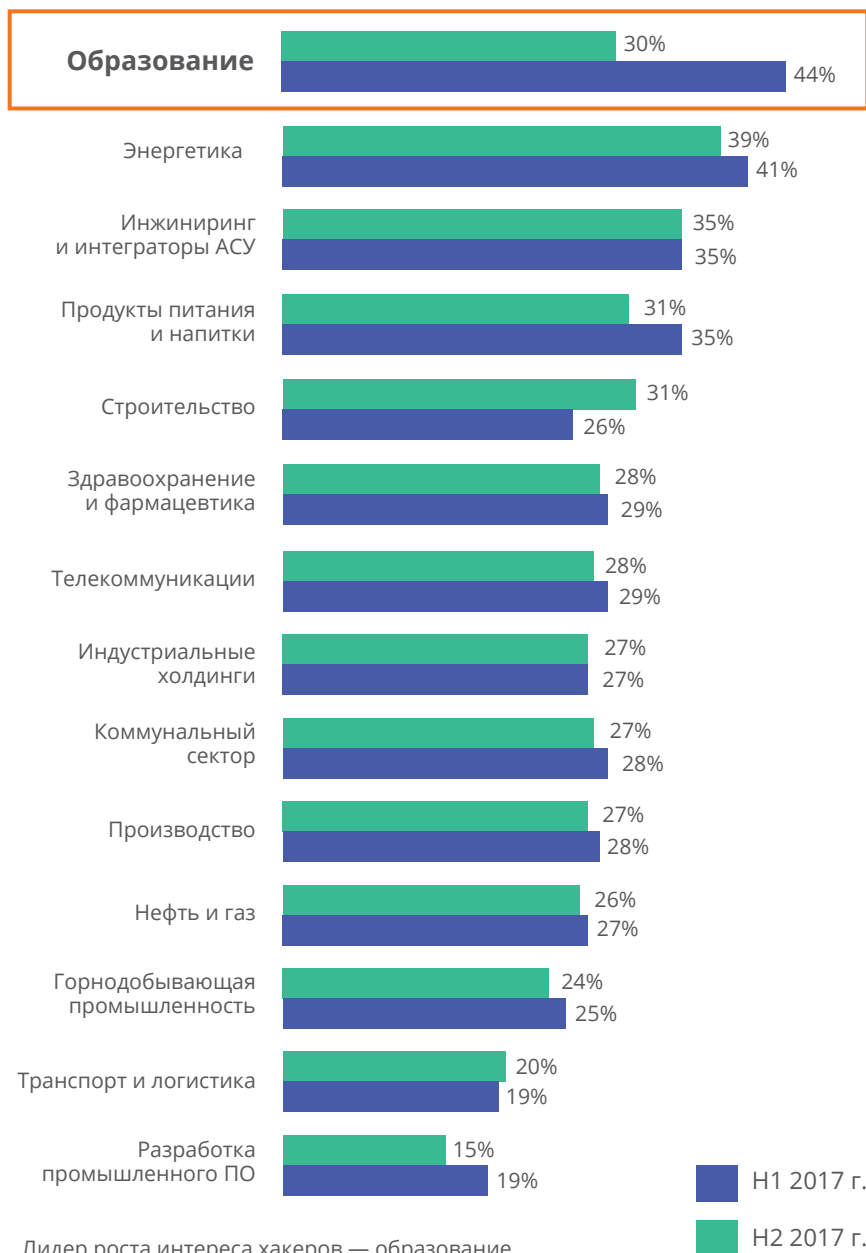
Эксперты «Лаборатории Касперского» подсчитали, что с сентября 2017 года по сентябрь 2018 года около 1000 фишинговых атак пришлось на сайты ведущих мировых университетов.

Целью мошенников был сбор конфиденциальных данных, включая результаты научных исследований во множестве областей: от экономики до ядерной физики.

Среди жертв хакеров — не только университеты, но и обычные общеобразовательные школы. Ученики взламывают компьютерную систему учебного заведения, чтобы подменить оценки.

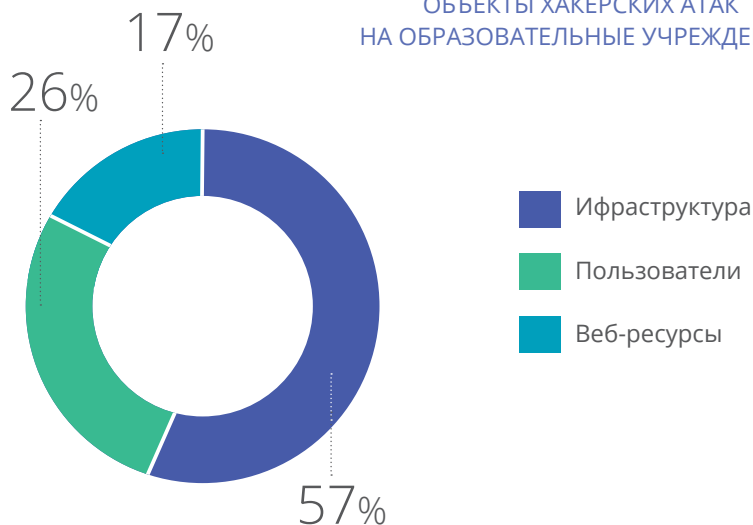
Опасны и внешние хакеры, нацеленные на персональные данные учащихся: адреса проживания, электронную почту родителей, места их работы и телефоны.

## ПРОЦЕНТ АТАКОВАННЫХ КОМПЬЮТЕРОВ АСУ В РАЗЛИЧНЫХ ИНДУСТРИЯХ, ПЕРВОЕ И ВТОРОЕ ПОЛУГОДИЯ 2017 ГОДА

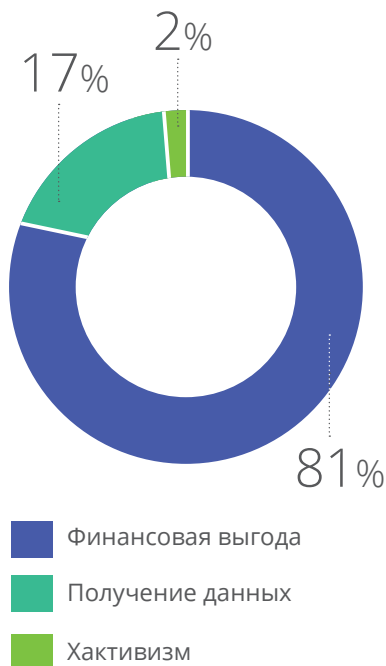


Источник: [www.ics-cert.kaspersky.ru/reports/2018/03/26/threat-landscape-for-industrial-automation-systems-in-h2-2017/](http://www.ics-cert.kaspersky.ru/reports/2018/03/26/threat-landscape-for-industrial-automation-systems-in-h2-2017/)

## ОБЪЕКТЫ ХАКЕРСКИХ АТАК НА ОБРАЗОВАТЕЛЬНЫЕ УЧРЕЖДЕНИЯ



## МОТИВЫ АТАК



## МЕТОДЫ АТАК

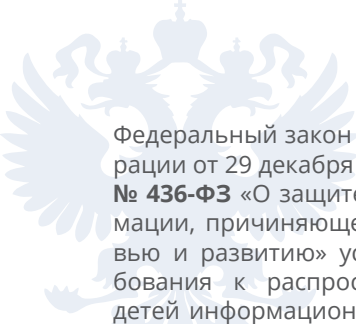


Источник: [www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2017-rus.pdf](http://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2017-rus.pdf)

# «Цифровые» законы

в образовании





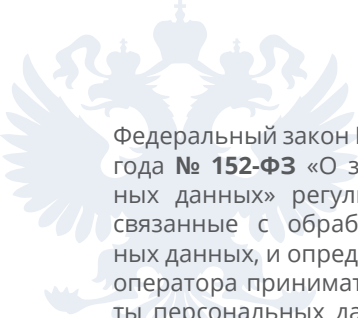
Федеральный закон Российской Федерации от 29 декабря 2010 г.

**№ 436-ФЗ** «О защите детей от информации, причиняющей вред их здоровью и развитию» устанавливает требования к распространению среди детей информационной продукции. В частности, закон определяет, что в местах, доступных для детей, организатор доступа в интернет обязан обеспечить информационную безопасность детей, применяя административные и организационные меры, технические и программно-аппаратные средства защиты детей от информации, способной нанести им вред, — провоцирующей на суицид, употребление наркотических средств, побуждающей к жестокости, пропагандирующей нетрадиционные сексуальные отношения, содержащей нецензурную брань, порнографию и т. д.

Нарушение 436-ФЗ, связанное с неприменением лицом, организующим доступ к распространяемой посредством информационно-телекоммуникационных сетей информации в местах, доступных для детей, административных и организационных мер, технических, программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и развитию, наказывается административным штрафом. Для лиц, осуществляющих предпринимательскую деятельность без образования юридического лица, в размере от 5 тысяч до 10 тыс. рублей; для юридических лиц — от 20 тысяч до 50 тыс. рублей (статья 6.17 КоАП РФ).

В июне 2017 года прокуратура Южноуральска обнаружила, что из-за отсутствия надлежащей контентной фильтрации в компьютерах кабинета информатики в трех школах города в свободном доступе для учащихся находятся материалы, включенные в Федеральный список экстремистских материалов.

По результатам рассмотрения представлений прокуратуры нарушения в школах устранены, трое виновных должностных лиц (преподаватели информатики) **привлечены к дисциплинарной ответственности.**



Федеральный закон РФ от 27 июля 2006 года № 152-ФЗ «О защите персональных данных» регулирует отношения, связанные с обработкой персональных данных, и определяет обязанность оператора принимать меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Требования к защите персональных данных при их обработке в информационных системах персональных данных утверждены Постановлением Правительства РФ от 01.11.2012 № 1119. В числе прочего они определяют необходимость использования средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства РФ в области обеспечения безопасности информации.

За нарушения законодательства, связанные с утечкой персональных данных, административные штрафы могут быть наложены как на организации и индивидуальных предпринимателей, так и на должностные лица, а также сотрудников, имеющих доступ к персональным данным.

В декабре 2017 года Большекаменская межрайонная прокуратура Приморского края обнаружила на компьютерах в городской детской библиотеке отсутствие контент-фильтров на компьютерах.

Прокурор вынес постановление о возбуждении дела об административном правонарушении по ч. 2 ст. 6.17 КоАП (неприменение лицом, организующим доступ к распространяемой посредством информационно-телекоммуникационных сетей информации в местах, доступных для детей, административных и организационных мер, технических, программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и (или) развитию). **Руководство библиотеки оштрафовано на 20 тыс. рублей.**



Согласно Постановлению Правительства РФ от 31 июля 2014 г. **№ 758** «О внесении изменений в некоторые акты Правительства Российской Федерации...», оказание универсальных услуг связи по передаче данных и предоставлению доступа в интернет с использованием пунктов коллективного доступа (публичных Wi-Fi-сетей) может осуществляться оператором универсального обслуживания только после идентификации пользователей.



В отношении юридических лиц штраф за несоблюдение требований законодательства достигает

**200**  
тыс. рублей

Постановлением Правительства РФ от 16 ноября 2015 г. **№ 1236** «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств...» утверждены правила формирования и ведения Единого реестра российских программ для ЭВМ и баз данных, а также определено, что госучреждения должны использовать российское программное обеспечение.

Приказом ФСТЭК России от 11.02.2013 **№ 17** утверждены Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Согласно требованиям, для обеспечения защиты такой информации должны применяться средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации (т. е. имеющие соответствующий сертификат ФСТЭК).

# Решение цифровых задач образовательных учреждений





**UTM-система** (Unified threat management) — универсальное решение защиты от сетевых угроз. Представляет собой шлюз безопасности корпоративных компьютерных сетей с функциями межсетевого экранирования, антивирусной проверки проходящего трафика, защиты от внешних вторжений (IDS/IPS), контентной фильтрации, VPN, мониторинга сетевой активности пользователей и другими возможностями. Эта технология пришла на смену межсетевым экранам (файерволам) как ответ на рост разнообразия кибератак.

### UTM-СИСТЕМЫ КОМПЛЕКСНО РЕШАЮТ СЛЕДУЮЩИЕ ЗАДАЧИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УЧЕБНЫХ ОРГАНИЗАЦИЙ



#### **Блокировка запрещенных ресурсов**

Блокируют ресурсы из черного списка Роскомнадзора и постоянно обновляют реестр запрещенных сайтов с портала [rkn.gov.ru](http://rkn.gov.ru).



#### **Блокировка вредного контента**

Блокируют страницы по стоп-словам, которые алгоритм находит в содержимом сайта. Система может заблокировать опасный контент, даже если сайт еще не добавлен в черный список Роскомнадзора.



#### **Нецелевое использование интернета**

Закрывают доступ в соцсети, видеохостинги, сайты знакомств, игровые порталы, онлайн-казино и т. п. Блокируют приложения (торренты, мессенджеры и т. п.). Блокируют рекламу на сайтах.



#### **Отражение атак на компьютерную сеть организации**

С помощью системы IDS/IPS обнаруживают и предотвращают неавторизованный доступ в локальную компьютерную сеть и защищают персональные данные от утечки.

## ДОПОЛНИТЕЛЬНЫЕ ПРЕИМУЩЕСТВА UTM-СИСТЕМ



### **Мониторинг действий учащихся в интернете**

дает руководству учебного учреждения следующие возможности:

- исходя из интересов аудитории организовывать секции, факультативы, кружки;
- выявлять и предотвращать критические ситуации, связанные с суицидом, агрессией и другими угрозами, направленными на учащихся и преподавателей.

Действия учащихся фиксируются системой как на компьютерах организации, так и на смартфонах, подключенных к сети Wi-Fi.



### **Антивирус**

на уровне шлюза проверяет весь проходящий трафик и защищает от заражения все компьютеры организации.



### **Балансировка трафика**

не дает «проседать» интернету даже при большом количестве активных подключений и низкой скорости провайдера.



### **SMS-идентификация**

пользователей в сети Wi-Fi позволяет соблюдать Постановление Правительства РФ от 31 июля 2014 г. № 758, которое вводит обязательную идентификацию пользователей публичных Wi-Fi-сетей.

# Почему учебные учреждения выбирают решения «СМАРТ-СОФТ»



Компания «Смарт-Софт» лицензирована Федеральной службой по техническому и экспортному контролю (ФСТЭК) на деятельность по разработке и производству средств защиты конфиденциальной информации.

Многофункциональный межсетевой экран Traffic Inspector FSTEC имеет сертификат соответствия ФСТЭК России № 2407 от 15.08.2011 года, удостоверяющий, что ПО является межсетевым экраном типа «Б» и соответствует требованиям документов «Требования к межсетевым экранам» (ФСТЭК России, 2016) и «Профиль защиты межсетевых экранов типа «Б» пятого класса защиты. ИТ.МЭ.Б5.ПЗ» (ФСТЭК России, 2016). Срок действия сертификата — до 15.08.2020 года.

Универсальный шлюз безопасности (UTM) Traffic Inspector Next Generation FSTEC имеет сертификат соответствия № 3834 от 04.12.2017 года, удостоверяющий, что программно-аппаратный комплекс является межсетевым экраном типа «А» и «Б» и соответствует требованиям документов «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа «А» четвертого класса защиты. ИТ.МЭ.А4.ПЗ» и «Профиль защиты межсетевых экранов типа «Б» четвертого класса защиты. ИТ.МЭ.Б4.ПЗ». Срок действия сертификата — до 04.12.2020 года.

Завершение сертификации антивирусной защиты и системы обнаружения (предотвращения) вторжений планируется в первом полугодии 2019 года.

## СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ  
№ РОСС RU.0001.01БИ00

### СЕРТИФИКАТ СООТВЕТСТВИЯ

№ 2407

Выдан 15 августа 2011 г.  
Действителен до 15 августа 2017 г.  
Срок действия продлен до 15 августа 2020 г.

Настоящий сертификат удостоверяет, что программный комплекс «Traffic Inspector 3.0», разработанный и производимый ООО «СМАРТ-СОФТ» в соответствии с техническими условиями ТУ 5015-003-13346898-16, функционирующий в средах операционных систем, указанных в формуляре 501590-003-13346898-16 ФО, является межсетевым экраном типа «Б», соответствует требованиям документов «Требования к межсетевым экранам» (ФСТЭК России, 2016) и «Профиль защиты межсетевых экранов типа «Б» пятого класса защиты. ИТ.МЭ.Б5.ПЗ» (ФСТЭК России, 2016).

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ОАО «Безопасность информационных технологий и компонентов» (аттестат аккредитации от 31.05.2003 № СЗИ RU.1190.2003.056) – техническое заключение от 24.01.2011, экспертного заключения от 21.07.2011 органа по сертификации ФАУ «НИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 26.04.2005 № СЗИ RU.840.A92.007) и результатов инспекционного контроля, проведенного испытательной лабораторией ОАО «Безопасность информационных технологий и компонентов» – техническое заключение от 20.07.2012, 21.06.2014, и испытательной лабораторией ЗАО «ДОКУМЕНТАЛЬНЫЕ СИСТЕМЫ» (аттестат аккредитации от 15.09.2016 № СЗИ RU.0001.01БИ00.0010) – техническое заключение от 30.03.2017.

Заявитель: ООО «СМАРТ-СОФТ»  
Адрес: 140408, Московская обл., г. Коломна, ул. Сапожниковых, д. 15  
Телефон: (495) 775-5991

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль ее соответствия требованиям документов, указанных в настоящем сертификате, осуществляется испытательной лабораторией ЗАО «ДОКУМЕНТАЛЬНЫЕ СИСТЕМЫ».

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ



В. Лютиков

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации  
15 августа 2011 г.

## СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ  
№ РОСС RU.0001.01БИ00

### СЕРТИФИКАТ СООТВЕТСТВИЯ

№ 3834

Выдан 4 декабря 2017 г.  
Действителен до 4 декабря 2020 г.

Настоящий сертификат удостоверяет, что программно-аппаратный комплекс «Traffic Inspector Next Generation» разработанный и производимый ООО «СМАРТ-СОФТ» в соответствии с техническими условиями ТУ 5015-003-13346898-16, является межсетевым экраном типа «А» и «Б», соответствует требованиям документов «Требования к межсетевым экранам» (ФСТЭК России, 2016) и «Профиль защиты межсетевых экранов типа А четвертого класса защиты. ИТ.МЭ.А4.ПЗ» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ» (ФСТЭК России, 2016) при выполнении указанных по эксплуатации, приведенных в формуляре 501590-003-13346898-16 ФО.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ЗАО «ДОКУМЕНТАЛЬНЫЕ СИСТЕМЫ» (аттестат аккредитации от 15.09.2016 № СЗИ RU.0001.01БИ00.0010) – техническое заключение от 07.09.2017, экспертного заключения от 17.11.2017 органа по сертификации ФАУ «НИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.A002).

Заявитель: ООО «СМАРТ-СОФТ» (ИНН 502022904)  
Адрес: 140408, Московская обл., г. Коломна, ул. Сапожниковых, д. 15  
Телефон: (495) 775-5991

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль ее соответствия требованиям документов, указанных в настоящем сертификате, осуществляется испытательной лабораторией ЗАО «ДОКУМЕНТАЛЬНЫЕ СИСТЕМЫ».

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ



В. Лютиков

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации  
4 декабря 2017 г.

**Traffic Inspector** и **Traffic Inspector Next Generation** занесены в Единый реестр российских программ для электронных вычислительных машин и баз данных.

Как найти решения «Смарт-Софт» в реестре:

1. Зайти на сайт Единого реестра: <https://reestr.minsvyaz.ru/reestr/>
2. В строку поиска ввести название нужного продукта (Traffic Inspector или Traffic Inspector Next Generation).
3. Вместо названия можно использовать общие слова: «межсетевой экран», «универсальный шлюз», «шлюз безопасности», «система обнаружения вторжений».

1

Единый реестр российских программ для электронных вычислительных машин и баз данных

Классы программного обеспечения

Название программного обеспечения (часть названия)

Правообладатель программного обеспечения

№ ↑ ↓    Название ↑ ↓    Класс ПО    Дата внесения ↑ ↓    Адрес сайта

2

Реестр Заявления Документы Помощь Личный кабинет

Главная / Реестр

## Единый реестр российских программ для электронных вычислительных машин и баз данных

Классы программного обеспечения: средства обеспечения информационной безопасности

Название программного обеспечения (часть названия):

Правообладатель программного обеспечения: Не выбран

Применить Сбросить

№ ↑ ↓ Название ↑ ↓ Класс ПО Дата внесения ↑ ↓ Адрес сайта

3

Реестр Заявления Документы Помощь Личный кабинет

Главная / Реестр / Traffic Inspector FSTEC

## Traffic Inspector FSTEC

### Сведения о правообладателях программного обеспечения

**Российская коммерческая организация**

Название организации: ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "СМАРТ-СОФТ"

ИНН: 5022032904

### Сведения об исключительном праве

Собственная разработка компании ООО «Смарт-Софт» (создание служебного произведения)

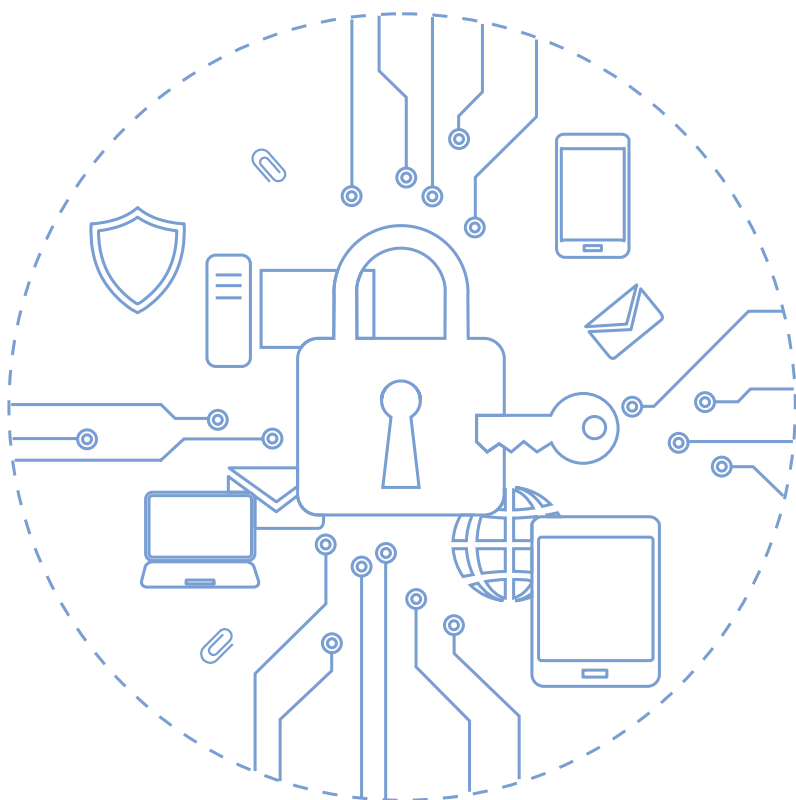
**Альтернативные наименования:**  
Трафик Инспектор ФСТЭК  
Traffic Inspector ФСТЭК  
Трафик Инспектор FSTEC

**Класс ПО:**  
средства обеспечения информационной безопасности

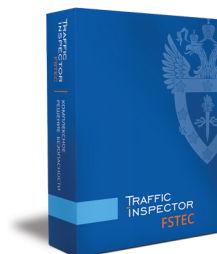
**Сайт производителя:**  
<http://smart-soft.ru/solutions/governmen>

**Дата решения**  
уполномоченного органа

# Решения «СМАРТ-СОФТ»



## TRAFFIC INSPECTOR FSTEC



### **Сертифицированный многофункциональный межсетевой экран**

Программный комплекс

Количество учетных записей:  
от 5 до 500 (максимальное  
количество пользователей  
зависит от характера трафика  
и используемой настройки  
функциональных модулей).

ОС Windows.

Сертификат соответствия  
ФСТЭК России № 2407 от  
15.08.2011 года.

Межсетевой экран типа «Б»,  
соответствует требованиям  
документов «Требования  
к межсетевым экранам» (ФСТЭК  
России, 2016) .

## TRAFFIC INSPECTOR NEXT GENERATION FSTEC



### **Сертифицированный универсальный шлюз безопасности (UTM)**

Программно-аппаратный ком-  
плекс

Количество учетных записей:  
до 100 пользователей (S 100), от  
100 до 500 пользователей (S 500),  
от 500 до 1000 (M 1000) и более  
1000 пользователей (L 1000+).

ОС FreeBSD.

Сертификат соответствия ФСТЭК  
России № 3834 от 04.12.2017  
года.

Программно-аппаратный  
комплекс является межсетевым  
экраном типа «А» и «Б» и соот-  
ветствует требованиям докумен-  
тов «Требования к межсетевым  
экранам» (ФСТЭК России, 2016).

## TRAFFIC INSPECTOR FSTEC

«Профиль защиты межсетевых экранов типа «Б» пятого класса защиты. ИТ.МЭ.Б5.ПЗ» (ФСТЭК России, 2016).

Срок действия сертификата — до 15.08.2020 года.

## TRAFFIC INSPECTOR NEXT GENERATION FSTEC

«Профиль защиты межсетевых экранов типа «А» четвертого класса защиты. ИТ.МЭ.А4.ПЗ» и «Профиль защиты межсетевых экранов типа «Б» четвертого класса защиты. ИТ.МЭ.Б4.ПЗ».

Срок действия сертификата — до 04.12.2020 года.

Завершение сертификации антивирусной защиты  
и системы обнаружения (предотвращения) вторжений (IDS/IPS)  
планируется в первом полугодии 2019 года.

### Где можно применять

- в государственных информационных системах второго класса защищенности (не работающих с государственной тайной);
- в автоматизированных системах управления производственными и технологическими процессами второго класса защищенности;
- в информационных системах персональных данных при необходимости обеспечения второго уровня защищенности персональных данных.

- в государственных информационных системах первого и второго класса защищенности;
- в автоматизированных системах управления производственными и технологическими процессами первого класса защищенности;
- в информационных системах персональных данных при необходимости обеспечения первого уровня защищенности персональных данных;
- в информационных системах общего пользования второго класса.

## ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

|                                                        |                                                |                                                                                                                          |                                                                                 |
|--------------------------------------------------------|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Краткое описание                                       |                                                | <p>Программный комплекс, который можно установить на уже имеющийся сервер или компьютер высокой производительности. Не требует приобретения дополнительного оборудования. Решение на базе ОС Windows.</p> | <p>Программно-аппаратный комплекс. В зависимости от количества сотрудников можно выбрать решения на 100, 500, 1000 и более лицензий. Решение на базе FreeBSD.</p> |
| Защита от атак                                         | Межсетевой экран (Firewall)                    | +                                                                                                                                                                                                         | +                                                                                                                                                                 |
|                                                        | VPN                                            | +                                                                                                                                                                                                         | +                                                                                                                                                                 |
|                                                        | Proxy                                          | +                                                                                                                                                                                                         | +                                                                                                                                                                 |
|                                                        | Система IDS/IPS                                | В процессе получения сертификата                                                                                                                                                                          |                                                                                                                                                                   |
| Фильтрация трафика и защита от нежелательного контента | Фильтрация с помощью правил межсетевого экрана | +                                                                                                                                                                                                         | +                                                                                                                                                                 |
|                                                        | Фильтрация веб-трафика                         | +                                                                                                                                                                                                         | +                                                                                                                                                                 |
|                                                        | Контентная фильтрация                          | Дополнительный модуль NetPolice                                                                                                                                                                           |                                                                                                                                                                   |
|                                                        | L7-фильтрация                                  | +                                                                                                                                                                                                         | +                                                                                                                                                                 |
|                                                        | Декодирование и проверка HTTPS-трафика         | +                                                                                                                                                                                                         | +                                                                                                                                                                 |

|                                                             |                                                                                                                       | Traffic Inspector<br>FSTEC | Traffic Inspector Next<br>Generation FSTEC |
|-------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|----------------------------|--------------------------------------------|
| Балансировка трафика                                        | Шейпер (ограничение скорости работы пользователей и групп)                                                            | +                          | -                                          |
|                                                             | Приоритизация трафика                                                                                                 | +                          | +                                          |
|                                                             | Переключение на запасные интернет-каналы (переключение происходит автоматически при выходе из строя основного канала) | +                          | +                                          |
|                                                             | Бриджинг Ethernet-интерфейсов                                                                                         | -                          | +                                          |
|                                                             | Распределение входящей сетевой нагрузки между несколькими обслуживающими серверами во внутренней сети                 | -                          | +                                          |
|                                                             | Балансировка исходящей нагрузки между несколькими WAN-подключениями                                                   | -                          | +                                          |
|                                                             | Кластер высокой доступности                                                                                           | -                          | +                                          |
|                                                             |                                                                                                                       |                            |                                            |
| Соблюдение «цифровых» законов РФ                            |                                                                                                                       | Блокировка контента 18+    | Блокировка контента 18+                    |
|                                                             |                                                                                                                       | Защита персональных данных | Защита персональных данных                 |
| Ведение учета посещаемости веб-ресурсов и активности в сети | Сетевая статистика                                                                                                    | +                          | На базе технологий NetFlow                 |
|                                                             | Отчет по пользователям, отчет по времени, отчет по скорости, отчет по активности пользователей                        | +                          | Отчеты и графики RRDtool                   |
|                                                             | Отчет антивируса                                                                                                      | +                          | +                                          |
|                                                             | Отчет веб-прокси                                                                                                      | +                          | +                                          |

|                                                             |                                                                                    | Traffic Inspector FSTEC                                                                                                             | Traffic Inspector Next Generation FSTEC                                                                          |
|-------------------------------------------------------------|------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Ведение учета посещаемости веб-ресурсов и активности в сети | Журнал действий системного администратора                                          | +                                                                                                                                   | +                                                                                                                |
|                                                             | Журнал сетевого экрана (в том числе фиксация попыток несанкционированного доступа) | -                                                                                                                                   | +                                                                                                                |
|                                                             | Системный журнал FreeBSD                                                           | -                                                                                                                                   | +                                                                                                                |
| Количество пользователей                                    |                                                                                    | От 5 до 500<br>(максимальное количество пользователей зависит от характера трафика и используемой настройки функциональных модулей) | В зависимости от модификации:<br>S 100 — до 100,<br>S 500 — до 500,<br>M 1000 — до 1000,<br>L 1000+ — более 1000 |



## ТЕХНИЧЕСКОМУ СПЕЦИАЛИСТУ

### Traffic Inspector Next Generation FSTEC

#### РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

[www.smart-soft.ru/support/documentation/handbook/ting/](http://www.smart-soft.ru/support/documentation/handbook/ting/)

#### СЦЕНАРИИ ВНЕДРЕНИЯ

[www.smart-soft.ru/support/documentation/scenario/ting\\_education.pdf](http://www.smart-soft.ru/support/documentation/scenario/ting_education.pdf)

### Traffic Inspector FSTEC

#### РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

[www.smart-soft.ru/support/documentation/handbook/ti/](http://www.smart-soft.ru/support/documentation/handbook/ti/)

#### БАЗА ЗНАНИЙ

[www.smart-soft.ru/support/documentation/kbase/](http://www.smart-soft.ru/support/documentation/kbase/)

# Истории внедрения



## ЗАДАЧИ

Руководством высшего учебного заведения была поставлена задача обеспечить локальную сеть (500 компьютеров) с единой точкой выхода в интернет, которая бы обеспечивала безопасное соединение и возможность блокировки доступа к сайтам. Мотивы руководства:

- сотрудники проводят много времени в социальных сетях, на сайтах знакомств и других нецелевых ресурсах;
- пользователи внутренней сети заходят на потенциально опасные внешние ресурсы;
- нецелевое использование интернета резко увеличило трафик, нагрузку на локальную сеть и расходы организации;
- растущая угроза хакерской атаки извне.

## РЕШЕНИЕ

Программно-аппаратный комплекс Traffic Inspector Next Generation наилучшим образом подошел под требования заказчика, поскольку обладает сертификатом ФСТЭК и всеми необходимыми функциями.

## РЕЗУЛЬТАТ

«Решение Traffic Inspector Next Generation FSTEC оказалось не только наиболее подходящим, но и самым выгодным: у конкурентов цена под нужное количество компьютеров оказалась выше в два-три раза!».

Франчук Тарас,  
инженер отдела ИБ университета

## ЗАДАЧИ

В школе 540 учеников, есть компьютерный кабинет и терминальный класс — в общей сложности в учреждении установлено 60 ЭВМ.

В 2009 году был проведен интернет (17 Мб/с), который уже четыре раза становился поводом для прокурорских проверок.

#### РЕШЕНИЕ

Превентивно, сразу после прокладки сети, был приобретен межсетевой экран Traffic Inspector. Установка заняла меньше одного дня и обошлась силами учителя информатики Слеменевой Татьяны Владимировны (по специальности Татьяна Владимировна — инженер-системотехник ЭВМ).

#### РЕЗУЛЬТАТ

По словам учителя, помимо прокурорских проверок, межсетевой экран успешно помогает решать другую задачу, возложенную на заведение, — подготовку ежеквартальных отчетов о том, какие сайты блокируются, а какие, наоборот, занесены в белые списки.

### ЩЕЛКОВСКИЙ КОЛЛЕДЖ В МОСКОВСКОЙ ОБЛАСТИ

#### ЗАДАЧИ

К локальной сети подключено 500 компьютеров, из них 200 — это рабочие места для студентов, численность которых превышает 2 тысячи. В 2017 году встал вопрос приобретения межсетевого экрана, сертифицированного ФСТЭК (до этого работало иностранное решение). Критерии — цена, функциональность, производительность.

#### РЕШЕНИЕ

После приобретения Traffic Inspector IT-отделу колледжа (коллективу из двух системных администраторов) понадобилось всего полдня на внедрение и настройки, без привлечения каких-либо внешних специалистов.

По словам представителя колледжа Алексея Летуновского, в службу поддержки не пришлось обращаться, хотя такая возможность изначально заявлялась производителем. На скорость интернета система почти не повлияла (местный провайдер обеспечивает выделенную линию 100 Мбит/с).

## РЕЗУЛЬТАТ

«К нам приходили с проверкой. После нее сотрудник прокуратуры пожал мне руку и сказал, что мы образцово-показательная организация», — говорит Алексей.

По словам специалиста, стоимость решения составила около 300 рублей в расчете на одного активного пользователя, что по соотношению цены и качества существенно выгоднее западных аналогов.

### ГИМНАЗИЯ № 8 ГОРОДСКОГО ОКРУГА КОЛОМНА МОСКОВСКОЙ ОБЛАСТИ

## ЗАДАЧИ

В начале 2015 года в гимназии встал вопрос создания новой локально-вычислительной сети с соблюдением законов РФ ФЗ-436 «О защите детей от информации, причиняющей вред их здоровью и развитию» и ФЗ-139 «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию».

## РЕШЕНИЕ

Специалисты «Смарт-Софта» предложили реализовать проект под ключ.

## РЕЗУЛЬТАТ

Организована новая локальная компьютерная сеть, установлено сертифицированное комплексное решение контроля и защиты интернет-доступа, подключен модуль контентной фильтрации, проведено обучение системного администратора.

### КРАСНОДАРСКИЙ ФИЛИАЛ ГОУ ВПО РОССИЙСКОГО ЭКОНОМИЧЕСКОГО УНИВЕРСИТЕТА ИМЕНИ Г. В. ПЛЕХАНОВА

## ЗАДАЧИ

Ключевой задачей для Краснодарского филиала университета являлось осуществление контроля сотрудников и предоставление качественного и бесперебойного доступа к интернету в учебных аудиториях.

Для обеспечения работы достаточно большой сети образовательного учреждения требовалось комплексное IT-решение, сочетающее универсальность, многофункциональность и простоту в использовании.

## РЕШЕНИЕ

Для решения задачи был выбран программный продукт Traffic Inspector, собственная разработка российской компании «Смарт-Софт».

Причины выбора:

- возможность применения хот-спота;
- возможность установки продукта на Windows;
- удобная и гибкая система фильтров;
- доступный механизм управления портами коммутаторов по проверке состояния баланса;
- оптимальное соотношение цены, качества и функциональности продукта.

## РЕЗУЛЬТАТ

После внедрения администрация вуза получила универсальное IT-решение, возможность распределять и осуществлять контроль сетевого трафика.

ГБПОУ «СОЧИНСКИЙ  
МЕДИЦИНСКИЙ КОЛЛЕДЖ»

## ЗАДАЧИ

В корпусах ГБПОУ «Сочинский медицинский колледж» учатся более 700 студентов. В учреждении четыре основные специальности, ответственность за обучение по которым на себя взял большой профессиональный педагогический коллектив. Колледж может похвастаться обширной методической библиотекой и собственной сетью с открытым доступом в интернет. Для контроля такой большой сети необходимо было подобрать комплексное решение, сочетающее универсальность, простоту и бесперебойную работу.

## РЕШЕНИЕ

Сеть Сочинского медицинского колледжа представлена одним сервером и 12 так называемыми «тонкими» клиентами.

Основная операционная система расположена на серверном ПК, а доступ каждого из двенадцати клиентов осуществляется через виртуальную среду vSpace Server. Основная проблема при интеграции сетевого экрана заключалась именно в настройке капризного клиентского оборудования.

Благодаря тому, что Traffic Inspector — гибкий сетевой инструмент, его тонкая настройка позволила избежать постоянно возникающих программных конфликтов, вызванных работой vSpace Server.

## РЕЗУЛЬТАТ

Администрация медицинского колледжа получила универсальное сетевое решение, обеспечивающее надежный контроль и защиту обширной компьютерной сети с возможностью фильтрации трафика.

В колледже был организован полный контроль над беспроводными сетями, представлен целый спектр сетевых инструментов для мониторинга активности и состояния сети, единый интуитивно понятный интерфейс.

# 5

## ФАКТОВ О КОМПАНИИ «СМАРТ-СОФТ»



### **Российский разработчик**

Разработка и техническая поддержка продуктов — в России.



### **Старше Facebook**

Первые строчки кода разработчики «Смарт-Софт» написали в 2003 году.



### **1 975 лицензий**

Максимальное количество лицензий, которое было приобретено одним заказчиком единовременно.



### **5 компьютеров**

Самая маленькая локальная сеть, которую защищает решение от «Смарт-Софта».



### **Анадырь**

Самый восточный город России, в котором работает клиент «Смарт-Софта». География внедрения решений «Смарт-Софта» включает все регионы России: от Анадыря на востоке до Калининграда на западе и от Певека на севере до Дербента на юге.



## ПОЛЕЗНЫЕ ССЫЛКИ

**Официальный сайт министерства просвещения РФ**

[www.edu.gov.ru](http://www.edu.gov.ru)

**Онлайн-медиа про образование и детей**

[www.mel.fm](http://www.mel.fm)

**Горизонты педагогики**

[www.pedgorizont.ru](http://www.pedgorizont.ru)

**Федеральный портал «Российское образование»**

[www.edu.ru](http://www.edu.ru)

**База учебных заведений**

[www.ucheba.ru](http://www.ucheba.ru)

**Рейтинг вузов**

[www.vuzoteka.ru](http://www.vuzoteka.ru)

**Каталог вузов**

[www.vuzopedia.ru](http://www.vuzopedia.ru)

## ПАМЯТКА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМНОМУ АДМИНИСТРАТОРУ



### Используйте антивирусы на уровне шлюза

Главный источник вирусов и прочего вредоносного кода — интернет. Установив антивирус на уровне шлюза, вы защитите сразу все компьютеры локальной сети, так как он проверяет проходящий через прокси-сервер трафик. Не забудьте прописать каждому пользователю в качестве прокси-сервера шлюз с антивирусом.

Госкомпаниям необходимо использовать решения, сертифицированные ФСТЭК, например антивирус «Лаборатории Касперского». Помимо него, в Traffic Inspector Next Generation можно использовать бесплатный плагин ClamAV, а также подключить другой антивирус, поддерживающий протокол ICAP.



### Используйте систему обнаружения/предотвращения вторжений (IDS/IPS)

Атаки на компьютерные сети организаций происходят в основном извне. Целью хакеров может стать как внешний ресурс (например, веб-сайт), так и внутренний (скажем, база данных). Решение — система обнаружения/предотвращения атак (IDS/IPS), которая распознает источники атак и атакуемые машины по определенным сигнатурам сетевого трафика и «очищает» трафик от подобных негативных воздействий. Кроме того, система оповещает администратора о происходящем и создает отчеты действий для того, чтобы по ним можно было провести расследование вторжений.

Как правило, функция IDS/IPS входит в состав универсальных UTM-систем информационной безопасности, причем не только дорогих западных, но и более доступных отечественных (читайте тест: [www.blog.smart-soft.ru/2018/09/19/testirovanie\\_sistemi\\_obnaruzheniya\\_vt/](http://www.blog.smart-soft.ru/2018/09/19/testirovanie_sistemi_obnaruzheniya_vt/)).



### Используйте прокси-сервер для фильтрации сетевого трафика

Часто системному администратору ставят задачу заблокировать нерегламентированные действия пользователей рабочих станций (просмотры видеороликов, общение в соцсетях, скачивание «пиратского» контента). Эти действия не только отнимают рабочее время, но и могут привести к заражению рабочей станции. Для предотвращения подобных действий на прокси-сервере необходимо установить правила блокировки доступа к определенным веб-ресурсам.

Полную версию инструкции читайте: [www.blog.smart-soft.ru/2019/03/25/pamyatka/](http://www.blog.smart-soft.ru/2019/03/25/pamyatka/)

## ПАМЯТКА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РУКОВОДИТЕЛЮ



### Не пренебрегайте официальными документами

Вышестоящие организации выпускают положения по обеспечению информационной безопасности, регламенты и т. п. Как правило, это малопонятные тексты, написанные канцелярским языком. Попросите системного администратора выделить из них суть и обсудите с ним реализацию главных поставленных задач.



### Следите за тем, чтобы сотрудники надежно хранили пароли

Доведите до персонала опасность раскрытия их паролей. Бумажка с шифром, приклеенная к монитору, даст хакеру ключ для взлома всей сети. Поставьте сотрудникам в обязанность менять пароли не реже чем раз в полгода (для наиболее важных сотрудников — раз в квартал).



### Распорядитесь о резервном копировании

Резервное копирование — это периодическая запись всех цифровых данных организации на внешний накопитель информации. В случае утраты рабочих данных их можно будет вернуть с помощью бэкапа. Как часто делать бэкапы и как долго их хранить? Оптимальный вариант — часто сохранять недавнюю информацию и долго хранить отдельные срезы, например делать бэкапы каждый день, хранить последние 30 дней, а также хранить срезы, сделанные 2, 3, 6, 12 и 24 месяца назад.



### Обучайте персонал информационной безопасности

Базовые вещи объяснит системный администратор, но желательно подходить к вопросу обучения комплексно, используя специальные курсы (например, Kaspersky ASAP). Для новых сотрудников сделать прохождение курсов обязательным.



### Проводите периодические проверки

Например, поставьте задачу системному администратору симулировать хакерскую атаку: отправить всем сотрудникам почтовое сообщение с подменой отправителя и «вирусным» файлом в архиве. Проведите разъяснительную работу среди тех, кто открыл опасное вложение.

## КОНТАКТЫ

тел.: +7 (495) 775-59-91, 8 (800) 511-05-81

e-mail: [info@smart-soft.ru](mailto:info@smart-soft.ru)

[www.smart-soft.ru](http://www.smart-soft.ru)