Приложение
к приказу
от **18.10.2018** № **1664-п**

Положение по антивирусной защите
ФГАОУ ВО «Севастопольский государственный университет»

1. Общие положения.

Настоящее «Положение по антивирусной защите ФГАОУ ВО «Севастопольский государственный университет» (далее - Университет)» (далее – Положение) определяет требования и ответственность при организации защиты информации от воздействия вредоносного кода.

Требования Положения распространяются на всех лиц, имеющих доступ к информационным системам Университета.

Термины и сокращения:

- АРМ – автоматизированное рабочее место;
- ЛВС – локальная вычислительная сеть;
- Отдел ИБ – Отдел информационной безопасности Управления информатизации и связи;
- ПО – программное обеспечение;
- УИС – Управление информатизации и связи;
- ФХД – финансово-хозяйственная деятельность.

2. Порядок использования средств антивирусной защиты.

2.1. Перечень антивирусного ПО, используемого в Университете, определяет УИС. При необходимости использования иного антивирусного ПО, такое решение согласовывается с начальником УИС, оформляется документально и хранится в УИС у ответственного за администрирование антивирусного ПО.

2.2. Подключение АРМ пользователей к ЛВС Университета без установленного антивирусного ПО запрещено.

2.3. Установку и настройку антивирусного ПО выполняют работники УИС, а также работники иных структурных подразделений Университета, которые допущены к установке и настройке антивирусного ПО распоряжением начальника УИС.

2.4. Антивирусное ПО, установленное на серверах и АРМ пользователей, должно иметь средства удалённого контроля работоспособности и обновления сигнатурных баз.

2.5. Одновременное использование нескольких средств антивирусной защиты разных производителей в одной операционной системе не допускается.

2.6. В антивирусном ПО должен быть постоянно включен резидентный модуль, выполняющий текущий «Контроль запуска программ», «Контроль активности программ», «Контроль устройств» и «Вэб-Контроль».

2.7. При невозможности использования резидентных модулей средств антивирусной защиты из-за особенностей технологического процесса либо конфигурации аппаратно-программных средств, их отключение осуществляется УИС и возможно только с разрешения начальника УИС.

2.8. Все электронные почтовые сообщения должны проходить обязательный автоматический контроль отсутствия вирусного заражения на почтовом сервере. В случае обнаружения на почтовом сервере вирусного заражения, передача зараженного электронного почтового сообщения должна автоматически блокироваться почтовым сервером, зараженное сообщение должно автоматически удаляться с почтового сервера.

2.9. Перед использованием обязательной полной проверке антивирусным ПО подлежат все отчуждаемые носители информации, которые перед этим использовались в устройствах, не принадлежащих Университету.

2.10. Установка ПО должна выполняться с дистрибутивов, которые заранее проверены на отсутствие вредоносного кода.

3. Требования к пользователю АРМ.

3.1. При работе в информационно-телекоммуникационной сети Университета пользователь обязан:

– ознакомиться с настоящим Положением;

– перед началом рабочего дня проверить работоспособность антивирусного ПО и обновление сигнатурных баз на своём АРМ в соответствии с «Краткой инструкцией по проверке работоспособности антивирусного ПО» (Приложение к настоящему Положению);

– сканировать антивирусным ПО подозрительные папки и файлы перед использованием;

– не отключать антивирусное ПО;

– не открывать файлы и не переходить по ссылкам из писем от неизвестных отправителей или писем с нетипичным для отправителя содержанием. При необходимости, связаться с работниками УИС;

3.2. При подозрении на вирусное заражение пользователь обязан:

– незамедлительно физически отключить АРМ пользователя от ЛВС Университета;

– выключить АРМ пользователя;

– незамедлительно поставить в известность о подозрении на вирусное заражение своего непосредственного руководителя и УИС любым доступным способом, в том числе:

Таблица 1

№ п/п	Способ обращения	Адресат обращения	Примечание
1	лично	ауд. А-105	ул. Университетская, д. 33
2	по телефону	1215 (88692) 417741 доб.1215	Перервин Владимир Юрьевич, начальник УИС
3		1224 (88692) 417741 доб.1224	Неугодников Юрий Васильевич, начальник Отдела ИБ УИС
4	по электронной почте	YVNeugodnikov@sevsu.ru VYPerervin@sevsu.ru	

– выполнять действия по устранению вирусного заражения, предписанные работниками УИС.

4. Требования к работнику УИС, ответственному за администрирование антивирусного ПО.

4.1. Работник УИС, ответственный за администрирование антивирусного ПО, назначается распоряжением начальника УИС.

4.2. Работник УИС, ответственный за администрирование антивирусного ПО, определяет требования к параметрам настроек антивирусного ПО, эксплуатируемого в Университете, в соответствии с требованиями настоящего Положения по согласованию с начальником УИС.

4.3. Работник УИС, ответственный за администрирование антивирусного ПО, должен осуществлять ежедневный контроль за работоспособностью антивирусного ПО, актуальностью сигнатурных баз, наблюдение за событиями на защищаемых антивирусным ПО АРМ пользователей.

4.4. Ежемесячно до 10 числа месяца, следующего за отчётным, работник, ответственный за администрирование антивирусного ПО, готовит

начальнику УИС отчёт о состоянии антивирусной защиты в Университете за отчётный месяц.

4.5. При обнаружении неработоспособного антивирусного ПО работник, ответственный за администрирование антивирусного ПО, сообщает об этом начальнику УИС, начальнику Отдела ИБ и предпринимает меры к восстановлению работоспособности антивирусного ПО. При невозможности восстановления работоспособности такой АРМ физически отключается от ЛВС Университета.

4.6. При подозрении на вирусное заражение работник, ответственный за администрирование антивирусного ПО:

– определяет факт наличия вируса, масштаб вирусного заражения;

– сообщает о факте вирусного заражения начальнику УИС, своему непосредственному начальнику, начальнику Отдела ИБ;

– предлагает способы устранения вирусного заражения;

– руководит действиями пользователей заражённых АРМ.

5. Ответственность.

5.1. Ответственность за организацию антивирусной защиты и текущий контроль её функционирования в Университете возлагается на начальника УИС.

5.2. Ответственность за организацию исполнения требований Положения в структурных подразделениях Университета, в том числе за ознакомление с ним пользователей АРМ, возлагается на руководителя структурного подразделения Университета.

5.3. Ответственность за исполнение требований Положения возлагается на пользователя АРМ.

6. Контроль.

Контроль исполнения требований Положения выполняют:

– начальник УИС при рассмотрении ежемесячных отчётов работника, ответственного за администрирование антивирусного ПО;

– Отдел ИБ.

Приложение
к Положению по антивирусной защите
ФГАОУ ВО «Севастопольский
государственный университет»

Краткая инструкция
по проверке работоспособности антивирусного ПО

1. Навести курсор мыши на значок антивируса Касперского в правом нижнем углу экрана (рисунок 1).

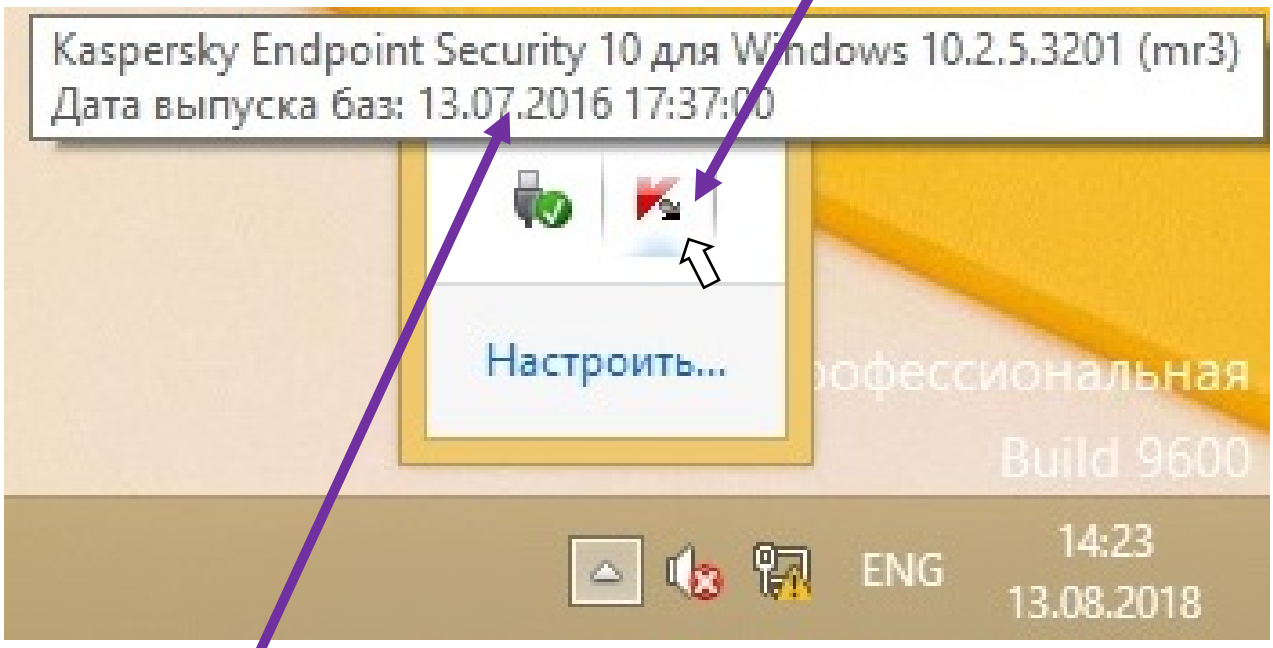

Рисунок 1.

2. Проверить дату выпуска баз в всплывающем окне.

3. Если «Дата выпуска баз» ранее, чем 7 дней назад, сообщить об этом в УИС по электронной почте на адрес YVNeugodnikov@sevsu.ru.