УТВЕЖДЕНА
приказом ФГАОУ ВО «СПбПУ»
от 28.11.2022 № 2709

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО»

ПОЛИТЕХ
Санкт-Петербургский
политехнический университет
Петра Великого

ПОЛИТИКА АНТИВИРУСНОЙ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ ФГАОУ ВО «СПбПУ»

Санкт-Петербург
2022 г.

1. Общие положения

1.1. Политика антивирусной защиты информационных ресурсов ФГАОУ ВО «СПбПУ» (далее – Политика) разработана в соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и приказом ФСТЭК от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.2. Требования настоящей Политики распространяются на всех работников федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский политехнический университет Петра Великого» (далее – ФГАОУ ВО «СПбПУ»).

1.3. Настоящая Политика определяет требования по защите информационных ресурсов (далее – ИР) ФГАОУ ВО «СПбПУ» от угроз информационной безопасности, причина возникновения которых связана с распространением вредоносного программного обеспечения (далее – ВПО). ИР – это совокупность информационных объектов (информации и ее носителей), которые находятся в распоряжении ФГАОУ ВО «СПбПУ» и могут быть использованы для осуществления деятельности ФГАОУ ВО «СПбПУ». Данные требования минимизируют вероятность возникновения негативных последствий для ИР ФГАОУ ВО «СПбПУ» вследствие отсутствия или неверного конфигурирования средств антивирусной защиты (далее – САВЗ). Негативные последствия могут включать в себя раскрытие или утрату конфиденциальных ИР, кражу интеллектуальной собственности, репутационные потери. Также Политика определяет ответственность должностных лиц за выполнение требований антивирусной защиты ИР и порядок эксплуатации САВЗ.

1.4. Политикой не охватываются вопросы защиты информационных систем, предназначенных для обработки информации, содержащей сведения, составляющие государственную тайну.

1.5. Политика подлежит регулярному пересмотру с периодичностью один раз в год для приведения системы антивирусной защиты в соответствие реальным условиям. Также может проводиться внеплановый пересмотр при изменении перечня решаемых задач, конфигурации технических и программных средств.

1.6. Контроль за исполнением требований настоящей Политики возлагается на начальника Управления информационной безопасности.

2. Требования к организации системы антивирусной защиты

2.1. Функционирование системы антивирусной защиты ИР реализуется в рамках единой системы защиты ИР ФГАОУ ВО «СПбПУ».

2.2. Система антивирусной защиты ИР предназначена для:

- предотвращения заражения серверного оборудования и автоматизированных рабочих мест (далее – АРМ) ВПО;
- обнаружения и безопасного устранения ВПО;
- предотвращения несанкционированных массовых почтовых рассылок и совершения противоправных действий, которые могут быть осуществлены с серверов и АРМ в случае заражения ВПО.

2.3. Антивирусная защита ИР осуществляется посредством применения организационных мер и САВЗ.

2.4. В целях обнаружения, предотвращения заражения и устранения ВПО в ФГАОУ ВО «СПбПУ» на постоянной основе должны использоваться САВЗ.

2.5. К использованию в информационных системах, входящих в состав ФГАОУ ВО «СПбПУ», допускаются САВЗ, имеющие необходимые лицензии и сертификаты.

2.6. Обязательному антивирусному контролю должны подлежать все файлы, получаемые и передаваемые по телекоммуникационным каналам, а также файлы на подключаемых машинных носителях информации.

2.7. Антивирусная защита ИР осуществляется централизованно. Для этой цели реализуется система антивирусной защиты ИР, включающая сервер централизованного администрирования (далее – антивирусный центр) и программы-агенты для установки на серверы и АРМ, обеспечивающие централизованный мониторинг и управление САВЗ.

2.8. Установка САВЗ осуществляется на все АРМ и серверы корпоративной вычислительной сети ФГАОУ ВО «СПбПУ». Также в обязательном порядке устанавливается агент управления САВЗ, который подключается к антивирусному центру, что обеспечивает централизованное управление: мониторинг состояния антивирусной защиты ИР, обновление, конфигурирование, периодическую регламентную проверку АРМ и серверов.

2.9. Пользователи информационных систем не должны иметь возможности получения доступа к конфигурации САВЗ или его отключения.

2.10. Пользователям запрещается отключать (удалять) САВЗ или агент удаленного управления САВЗ.

2.11. При установке программного обеспечения на серверы информационных систем и АРМ или их обновлении должна автоматически выполняться предварительная проверка данного программного обеспечения на отсутствие ВПО.

2.12. Функционирование системы антивирусной защиты ИР осуществляется непрерывно.

2.13. В случае обнаружения зараженных ВПО файлов пользователь обязан:

- приостановить работу;
- поставить в известность о факте обнаружения заражения файлов ВПО Управление информационной безопасности.

3. Ответственность за выполнение требований антивирусной защиты

3.1. Управление информационной безопасности несет ответственность за:

– разработку положений, инструкций, форм служебных записок (заявок) по процессам организации антивирусной защиты ИР;

– планирование мероприятий по антивирусной защите ИР;

– определение потребностей, закупку САВЗ и ежегодное продление лицензий;

– анализ состояния системы антивирусной защиты ИР;

– периодический контроль соблюдения требований к организации системы антивирусной защиты ИР, хранящихся или обрабатываемых в информационных системах Университета;

– проведение служебных проверок по фактам заражения ВПО ИР, хранящихся или обрабатываемых в информационных системах ФГАОУ ВО «СПбПУ»;

– проведение разъяснительных и консультационных работ с пользователями информационных систем в части использования САВЗ;

– разработку предложений о совершенствовании системы антивирусной защиты ИР.

3.2. Реализация исполнения требований и технических мероприятий, установленных настоящей Политикой, осуществляется работниками структурных подразделений ФГАОУ ВО «СПбПУ», ответственными за защиту ИР, в соответствии с их должностными инструкциями и другими внутренними документами ФГАОУ ВО «СПбПУ» по информационной безопасности.

3.3. Управление цифровых технологий оказывает техническую поддержку проведения работ по антивирусной защите ИР в зоне своей ответственности.

3.4. Начальник структурного подразделения осуществляет организацию и непосредственное руководство проведением работ по антивирусной защите ИР в зоне своей ответственности и выполняет:

– назначение ответственного за выполнение установки и конфигурации САВЗ;

– контроль проведения работ по обеспечению структурного подразделения САВЗ;

– предоставление отчетности о проделанной работе по обеспечению структурного подразделения САВЗ.

3.5. Персональную ответственность за соблюдение установленных норм обеспечения антивирусной защиты ИР на своих АРМ, в том числе за своевременное информирование работников Управления информационной безопасности о получении предупреждающих сообщений от установленных САВЗ, несут пользователи АРМ.

4. Порядок эксплуатации средств антивирусной защиты

4.1. Установку САВЗ на АРМ и серверы в зоне ответственности структурных подразделений производят работники, назначенные руководителем структурного подразделения, при технической поддержке службы поддержки пользователей.

4.2. Порядок установки САВЗ, агента управления САВЗ и порядок подключения его к антивирусному центру определяются Управлением информационной безопасности.

4.3. Порядок эксплуатации САВЗ устанавливается с учетом обязательного соблюдения:

– проверки на отсутствие ВПО для всех файлов на машинных носителях информации перед началом работы с ними;

– проверки всех электронных писем на предмет отсутствия ВПО;

– еженедельной проверки на предмет отсутствия ВПО на жестких магнитных дисках АРМ и серверов;

– внеплановой проверки любых машинных носителей информации и средств вычислительной техники в случае подозрения на наличие ВПО;

– восстановления работоспособности программных средств и файлов, поврежденных ВПО.

4.4. Обновление антивирусных баз на АРМ и серверах производится в автоматическом режиме ежечасно с серверов обновления разработчика САВЗ или с сервера администрирования антивирусной защиты. На АРМ пользователей, не имеющих подключения к корпоративной сети, подключение к антивирусному центру не производится, установка, настройка, антивирусных баз осуществляется локально.

4.5. Антивирусный центр обеспечивает:

– удаленную установку и обновление САВЗ;

– управление конфигурацией всего программного обеспечения системы антивирусной защиты;

– управление установкой и обновлением лицензионных ключей САВЗ;

– обеспечение обновления антивирусных баз на АРМ и серверах, подключенных к корпоративной вычислительной сети, но не имеющих доступа к сети Интернет;

– ограничение доступа пользователей на АРМ к настройкам САВЗ;

– настройку рассылки сообщений об обнаружении вирусов, о сбоях в работе САВЗ и т. п.;

– удаленное решение проблем, возникающих в процессе эксплуатации САВЗ.

4.6. Начальник Управления информационной безопасности ежемесячно представляет проректору по информационным технологиям доклад о состоянии антивирусной защиты ИР и вирусной активности в корпоративной вычислительной сети ФГАОУ ВО «СПбПУ».