ЧАСТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«СТАВРОПОЛЬСКИЙ КООПЕРАТИВНЫЙ ТЕХНИКУМ»

СОГЛАСОВАНО
Протокол заседания
Студенческого совета
от «30» августа 2023 г. № 1
Председатель Совета
_____

УТВЕРЖДАЮ
Директор Частного профессионального
образовательного учреждения
«Ставропольский кооперативный техникум»
_____А.А. Намитоков
от «30» августа 2023 г. Приказ № 112

ИНСТРУКЦИЯ

о защите информации о событиях безопасности в информационной системе персональных данных «Автоматизированное рабочее место оператора УОП»

Настоящая Инструкция определяет требования по защите информации о событиях безопасности в информационной системе персональных данных «Автоматизированное рабочее место оператора УОП» (далее - ИСПДн).

События безопасности, подлежащие регистрации в ИСПДн, определяются с учетом способов реализации угроз безопасности информации. К событиям безопасности, подлежащим регистрации в ИСПДн, относятся любые проявления состояния информационной системы и ее системы защиты персональных данных, указывающие на возможность нарушения конфиденциальности, целостности или доступности информации, доступности компонентов ИСПДн, нарушения процедур, установленных организационно-распорядительными документами по защите информации, а также нарушения штатного функционирования средств защиты информации.

В ИСПДн определены следующие события безопасности, подлежащие регистрации:

1. События, связанные с регистрацией входа (выхода) субъектов доступа в систему или загрузки операционной системы. Состав и содержание информации включают дату и время входа (выхода) в систему (из системы) или загрузки операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа.

2. События, связанные с регистрацией подключения машинных носителей информации и вывода информации на носители информации. Состав и содержание регистрационных записей включает: дату и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, подключившего машинный носитель или осуществляющего вывод информации на носитель информации.

3. События, связанные с регистрацией запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации. Состав и содержание регистрационных записей включает: дату и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный).

4. События, связанные с регистрацией попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. Состав и содержание регистрационных записей включает: дату и время попытки доступа к защищаемому файлу с указанием ее

5. События, связанные с регистрацией попыток доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам). Состав и содержание информации должны включать: дату и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого объекта доступа (логическое имя (номер).

6. События, связанные с регистрацией запланированного обновления антивирусных баз. Состав и содержание информации должны включать дату и время обновления.

7. События, связанные с регистрацией запланированного обновления ОС Windows. Ведутся в журнале самой ОС. Состав и содержание информации должны, включать дату и время обновления, состав обновления.

События безопасности, подлежащие регистрации в ИСПДн, и сроки хранения соответствующих записей регистрационных журналов, обеспечивают возможность обнаружения, идентификации и анализа инцидентов, возникших в ИСПДн.

Перечень событий безопасности, регистрация которых осуществляется в текущий момент времени, определяется Администратором безопасности, исходя из возможностей реализации угроз безопасности информации.

Срок хранения информации о зарегистрированных событиях безопасности должен составлять не менее трех месяцев, если иное не установлено требованиями законодательства Российской Федерации.

Защита информации о событиях безопасности (записях регистрации (аудита)) обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, определенных в соответствии с методическими документами, и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

Доступ к записям аудита и функциям управления механизмами регистрации (аудита) средств защиты информации (далее - СЗИ) предоставляется только Администратору безопасности ИСПДн.

В ИСПДн для обеспечения защиты информации о событиях безопасности, перед установкой СЗИ осуществляется синхронизация системного времени и даты. Администратор безопасности осуществляет контроль неизменности установленного системного времени и проводит периодическую проверку журналов регистрации событий, для контроля правильности отображения временных меток.

Сбор, запись и хранение информации о событиях безопасности осуществляется с помощью встроенных средств операционной системы Windows и установленных СЗИ.

В целях предотвращения сбоев при регистрации событий безопасности СЗИ и операционной системы в ИСПДн:

1. Администратору безопасности ИСПДн необходимо еженедельно проверять журналы регистрации событий СЗИ и операционной системы на наполненность и, в случае необходимости, производить их архивацию.

2. Увеличить при необходимости объем выделяемой под журналы событий безопасности СЗИ и операционной системы памяти.

3. Включить автоматическую перезапись новых событий безопасности поверх устаревших для предотвращения возникновения ошибок переполнения журналов.

4. Настройки прав учетных записей пользователей ИСПДн должны исключать

возможность внесения пользователями изменений в журналы событий безопасности, настройки СЗИ и операционной системы.

5. При появлении в ИСПДн ошибок операционной системы или СЗИ пользователю необходимо уведомить администратора безопасности и приостановить работу до устранения ошибки.