УТВЕРЖДАЮ
Директор ГБПОУ НХТК

_____ А.П. Москвитин
«25» 01 2018 г.

РЕГЛАМЕНТ

аудита и регистрации событий безопасности в сегментах государственных информационных систем ГБПОУ НХТК

1. Определения

1.1 Несанкционированный доступ – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

1.2 Администратор информационной безопасности – это субъект доступа, ответственный за защиту информационной системы от несанкционированного доступа к обрабатываемой в ней информации.

1.3 Событие информационной безопасности – идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики информационной безопасности или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.

2. Общие положения

2.1 Настоящий регламент разработан в соответствии с приказом ФСТЭК России № 17 от 11.02.2013 г. «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», а также методического документа ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержденного Федеральной службой технического и экспортного контроля России 11.02.2014 г.

2.2 Регламент определяет правила и объёмы аудита, сроки и порядок хранения, а также порядок защиты информации о событиях безопасности.

2.3 Контроль за исполнением настоящего регламента осуществляет ответственный за организацию защиты информации в сегментах ГИС государственного бюджетного профессионального образовательного учреждения «Невинномысский химико-технологический колледж» (далее – Учреждения).

3. Назначение и область действия

3.1 Данный регламент предназначен для администратора информационной безопасности сегмента ГИС.

3.2 Данный регламент распространяется на все сегменты ГИС Учреждения.

4. События безопасности, подлежащие регистрации

4.1 В Учреждении определяются следующие события безопасности, подлежащие аудиту:

1) вход/выход пользователя в сегмент ГИС. Необходимо регистрировать успешные и неуспешные попытки входа, время таких попыток, результат входа/выхода, а также при возможности технической реализации – предъявленный идентификатор (учетная запись, смарт-карта) и пароль;

2) доступ к ресурсам и/или информации сегмента ГИС. Необходимо осуществлять аудит доступа к информационным ресурсам (базы данных, файлы, содержащие защищаемую информацию и т.д.);

3) события, связанные с функционированием средств защиты информации;

4) события доступа в информационную систему из внешних информационно-телекоммуникационных сетей. Необходимо осуществлять регистрацию неуспешных попыток сетевого доступа к сегменту ГИС на межсетевом экране;

5) события средств антивирусной защиты. Необходимо осуществлять регистрацию результатов сканирования АРМ и серверов на предмет обнаружения вирусов и вредоносного ПО;

5. Сроки хранения событий безопасности

5.1 В организации устанавливаются следующие сроки хранения информации о событиях безопасности:

– журнал аудита операционной системы – не менее 3 месяцев;

– журнал аудита средства защиты от несанкционированного доступа – не менее 3 месяцев;

– журналы средств антивирусной защиты – не менее 3 месяцев;

– журналы межсетевых экранов / систем обнаружения вторжений – не менее 3 месяцев.

5.2 При возможности технической реализации необходимо производить архивирование журнала событий безопасности.

6. Защита информации о события безопасности

6.1 Доступ к информации о событиях безопасности должен иметь только администратор информационной безопасности организации.

6.2 Для обеспечения сохранности от подмены архивы с информацией о событиях безопасности должны хранится на неперезаписываемых устройствах хранения информации (например, CD-R, DVD-R) или должны быть зашифрованы с использованием средств криптографической защиты информации.

7. Пересмотр набора событий безопасности, подлежащих регистрации

7.1 Чтобы убедиться в том, что текущий набор событий по-прежнему необходим и достаточен, периодически должны осуществляться пересмотр и обновление набора событий безопасности.

7.2 Обязательно осуществляются пересмотр и обновление набора событий безопасности, подвергаемых аудиту при:

– проведении работ по модернизации сегмента ГИС;

– внедрении новых информационных технологий;

– проведении процедуры оценки эффективности.

8. Мониторинг результатов регистрации событий

8.1 Мониторинг результатов событий безопасности осуществляет администратор информационной безопасности организации.

8.2 Просмотр и анализ результатов событий безопасности осуществляется ежедневно.

8.3 При возникновении нештатной ситуации просмотр и анализ результатов событий безопасности осуществляется безотлагательно.

Начальник отдела автоматизации О. А. Просвирина