Приложение 6
к приказу директора
ГБПОУ КК УТМиПТ
от 27.03.2024 г. № 66

ПОЛИТИКА
аудита информационной безопасности государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий»

1. Общие положения

1.1. Настоящая политика аудита информационной безопасности (далее – Политика) государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий» (далее – образовательная организация) определяет объекты и периодичность проверки функционирования системы информационной безопасности.

1.2. Настоящая Политика разработана в соответствии с:

1.2.1 приказом Федеральной службы по техническому и экспортному контролю России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

1.2.2 приказом Федеральной службы по техническому и экспортному контролю России 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;

1.2.3 методическим документом Федеральной службы по техническому и экспортному контролю России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах».

2. Цели и задачи внутреннего аудита информационной безопасности

2.1 Основными целями проведения аудита информационной безопасности являются:

2.1.1 оценка текущего уровня защищённости информационных систем;

2.1.2 выявление и локализация уязвимостей в системе защиты информационных систем;

2.1.3 анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении информационных ресурсов;

2.1.4 оценка соответствия информационных систем требованиям Политики использования информационных активов государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий»;

2.1.5 выработка рекомендаций по совершенствованию системы управления информационной безопасностью за счёт внедрения новых и повышения эффективности существующих мер защиты информации.

2.2 В число задач, решаемых при проведении аудита информационной безопасности входят:

2.2.1 сбор и анализ исходных данных об организационной и функциональной структуре информационных систем, необходимых для оценки состояния информационной безопасности;

2.2.2 анализ существующей политики информационной безопасности и других организационно-распорядительных документов по защите информации на предмет их полноты и эффективности, а также формирование рекомендаций по их разработке (или доработке);

2.2.3 технико-экономическое обоснование механизмов информационной безопасности;

2.2.4 проверка правильности подбора и настройки средств защиты информации, формирование предложений по использованию существующих и установке дополнительных средств защиты для повышения уровня надёжности и безопасности информационных систем;

2.2.5 разбор инцидентов информационной безопасности и минимизация возможного ущерба от их проявления.

3. Проведение аудита информационной безопасности

3.1 Образовательная организация своими силами проводит внутренние проверки информационной безопасности через запланированные интервалы времени.

3.2 Внутренний аналитический аудит проводится Администратором информационных систем совместно с Администратором информационной безопасности.

3.3. Аудит информационной безопасности проводится ежегодно в соответствии с планом проведения внутреннего аудита информационной безопасности.

Аудит информационной безопасности структурных подразделений образовательной организации проводится ежеквартально в соответствии с планом проведения внутреннего аудита информационной безопасности.

Формы планов проведения внутреннего аналитического аудита информационной безопасности приведены в приложении 1 и 2 настоящей Политики.

3.4 По результатам проведенной проверки составляется план устранения недостатков, выявленных в ходе проведения аналитического аудита информационной безопасности. Форма плана приведена в приложении 3 настоящей Политики.

3.5 Работники образовательной организации при проведении у них аудита информационной безопасности обязаны оказывать содействие аудиторам и предоставлять всю необходимую для проведения аудита информацию.

Приложение 1
к политике аудита
информационной безопасности
министерства образования,
науки и молодежной политики
Краснодарского края

ФОРМА ПЛАНА
проведения ежегодного внутреннего аналитического аудита информационной безопасности государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий» науки и молодежной политики Краснодарского края

№ п/п	Объекты проверки	Результаты проверки	Примечание[1)]
1	2	3	4
1	**Назначение ответственных лиц**		
1.1	Проверка назначения администратора информационных систем		
1.2	Проверка назначения администратора информационной безопасности		
2	**Инвентаризация и учет информационных ресурсов (систем), средств обработки информации**		
2.1	Проверка наличия заполненных форм учета информационных ресурсов (систем), средств обработки информации и степени их актуальности:		
2.1.1	Учет информационных ресурсов и информационных систем		Проверяется, в том числе, корректность установленных классов защищенности (подтвержденных

[1)] Если требование не применимо к проверяемому подразделению – в графе «результаты проверки» делается соответствующая запись. В графе «примечание» указываются комментарии по результату оценки объекта проверки.

1	2	3	4
			актами классификации) и обоснованность критичности
2.1.2	учета автоматизированных рабочих мест		
2.1.3	учета серверов		
2.1.4	учета сетевого оборудования		
2.1.5	учета съемных носителей информации		
2.1.6	учета средств защиты информации		
2.2	Проверка наличия разработанных технических паспортов на информационные системы и степени их актуальности		
2.3	Проверка наличия разработанных описаний технологического процесса обработки информации в информационной системе и степени их актуальности		
3	**Эксплуатация и предоставление прав доступа к информационным ресурсам (системам), средствам обработки информации**		
3.1	Проверка наличия заявок на предоставление (изменение) прав доступа к информационным ресурсам (системам), средствам обработки информации, матрицы доступа и их соответствие реально имеющимся правам		
3.2	Проверка перечня используемых для доступа к АРМ учетных записей пользователей с фактическими использованными для доступа к АРМ		
3.3	Выборочная проверка отсутствия активных (незаблокированных) учетных записей уволенных сотрудников		
3.4	Выборочная проверка наличия минимальных прав доступа у заблокированных учетных записей		
3.5	Проверка на АРМ пользователей и серверах наличия информации (в том числе в истории интернет-браузеров), не относящейся к служебным обязанностям		
3.6	Проверка состава, используемого на АРМ пользователей и сервере программного обеспечения (в соответствии с Реестром разрешенного к использованию ПО)		
3.7	Проверка наличия печатей (пломб) на АРМ и серверах		
3.8	Проверка наличия установленных на АРМ и серверах паролей на доступ к BIOS		
3.9	Проверка возможности использования на АРМ пользователей технологий беспроводной передачи данных, веб-камер и микрофонов		
3.10	Проверка работоспособности на АРМ и серверах средств защиты информации		
3.11	Проверка наличия действующих сертификатов соответствия ФСТЭК России, выданных на используемые средства защиты информации		

1	2	3	4
3.12	Проверка настроек программного обеспечения и средств защиты информации требованиям эксплуатационной документации		Проверяется, в том числе, актуальность антивирусных баз
3.13	Проверка АРМ и серверов на предмет подключения к ним мобильных устройств передачи информации (в ретроспективе), а также неучтенных съемных носителей информации		
4	**Учет и использование съемных носителей информации**		
4.1	Проверка журнала учета выдачи съемных носителей информации с фактическим наличием у сотрудников данных съемных носителей		
4.2	Проверка наличия перечня мест хранения съемных носителей, назначения ответственных за них лиц и степени их актуальности		
4.3	Проверка съемных носителей информации на предмет наличия информации, не связанной с исполнением служебных обязанностей		
4.4	Проверка выполнения уничтожения (стирания) информации со съемных носителей информации		
4.5	Проверка выполнения порядка уничтожения съемных носителей информации		
5	**Эксплуатация аттестованных по требованиям безопасности информации информационных систем**		
5.1	Проверка наличия аттестата соответствия на информационные системы, выданного лицензиатом ФСТЭК России, и срока его действия		
5.2	Проверка выполнения порядка действий в ходе эксплуатации аттестованной информационной системы		Проверяется в случае обнаружения расхождений между техническим паспортом информационной системы сведениями, указанными в аттестационной документации, и реальным состоянием информационной системы
6	**Использование аутентификационной информации при доступе к информационным ресурсам (системам), средствам обработки информации**		
6.1	Проверка формата задания имен доступа пользователей установленным требованиям		
6.2	Проверка отсутствия гостевых учетных записей для доступа к АРМ, серверам, активному сетевому оборудованию, средствам защиты информации		
6.3	Выборочная проверка реализации требований, установленных к качеству аутентификационной информации и мер по обеспечению ее безопасности		После проверок исполнения требований к качеству пароля

1	2	3	4
			(приводящие к его санкционированной компрометации), пользователь должен продемонстрировать установленный пароль на доступ, после чего незамедлительно его сменить
6.4	Отсутствие сохраненных паролей доступа как на средствах программного обеспечения, так и на бумажных носителях (вне отведенных для этого мест)		
6.5	Проверка исполнения требований, предъявляемых к учету и использованию дополнительных средств аутентификации		При их использовании
7	**Организация доступа в помещения обработки информации и выполнение требований, установленных к таким помещениям**		
7.1	Проверка наличия перечня помещений, в которых разрешена обработка конфиденциальной информации (в том числе персональных данных) и степени его актуальности		
7.2	Проверка наличия перечня лиц, допущенных в помещения обработки конфиденциальной информации, степени его актуальности		Проверка наличия перечней для каждого помещения, а также в ходе проведения аудита проверяется степень исполнения данного требования при доступе в помещения
7.3	Проверка реализации требований, предъявляемых к помещениям обработки конфиденциальной информации:		
7.3.1	наличие ограждающих конструкций, предполагающих существенные трудности для нарушителей по их преодолению (металлические решетки на окнах, металлическая дверь, система контроля и управления доступом и так далее)		
7.3.2	надежные входные двери с замками, а также средствами опечатывания помещений		
7.3.3	окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в помещения посторонних лиц, оборудованы металлическими решетками или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в помещения		
7.4	Проверка наличия перечня мест хранения материальных носителей		

1	2	3	4
	персональных данных и ответственных лиц, степени актуальности данного перечня		
7.5	Проверка реализации дополнительных требований, предъявляемых к спецпомещениям:		
7.5.1	оборудованы устройствами, обеспечивающими постоянное закрытие дверей на замок и их открытие только для санкционированного прохода		
7.6	Проверка наличия журнала учета хранилищ СКЗИ и ключей от них, а также степени его актуальности		
8	**Защита технических средств от внешних воздействий**		
8.1	Способ реализации учета доступа в помещения		Указывается реализованный способ
8.2	Проверка наличия средств обеспечения температурно-влажностного режима серверных помещений		
8.3	Проверка наличия средств обеспечения бесперебойного резервного питания для АРМ		
8.4	Проверка наличия средств обеспечения бесперебойного резервного питания для серверов		
8.5	Проверка наличия средств обеспечения бесперебойного резервного питания для активного сетевого оборудования		
9	**Обеспечение отказоустойчивости технических средств**		
9.1	Проверка резервирования средств обработки информации, имеющих высокую критичность и способа резервирования		Указать способ резервирования
9.1.1	АРМ		
9.1.2	серверов		
9.1.3	активного сетевого оборудования, в том числе средств защиты информации, выполненных в виде программно-аппаратных комплексов		
9.2	Проверка наличия контроля основных показателей функционирования технических средств (степени загрузки: процессорных мощностей, дискового пространства, оперативной памяти, каналов связи и прочее)		Указать, какие показатели контролируются какими средствами
10	**Резервное копирование защищаемой информации**		
10.1	Проверка наличия заполненного перечня информационных ресурсов, подлежащих резервному копированию, его полноту и степень актуальности		
10.2	Проверка ведения журнала проведения резервного копирования информации		
10.3	Проверка ведения журнала восстановления информации		

1	2	3	4
10.4	Проверка мест хранения резервных копий		
11	**Учет и использование средств криптографической защиты информации**		
11.1	Проверка условий эксплуатации СКЗИ, в том числе выполнение требований эксплуатационной документации на СКЗИ		
11.2	Проверка журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов, степени его актуальности		
11.3	Проверка технического (аппаратного) журнала, степени его актуальности		
11.4	Проверка порядка уничтожения криптографических ключей (ключевой информации)		
12	**Обработка персональных данных**		
12.1	Проверка наличия размещенных на информационном интернет-портале министерства «Правил обработки персональных данных»		
12.2	Проверка степени актуальности уведомления об обработке персональных данных, поданных в Роскомнадзор		
12.3	Проверка наличия перечня обрабатываемых персональных данных и степени его актуальности		
12.4	Проверка наличия перечня должностей, замещение которых предусматривает осуществление обработки персональных данных, степени его актуальности		
12.5	Проверка наличия перечня информационных систем, в которых осуществляется обработка персональных данных		
12.6	Проверка соблюдения требований по учету и реагированию на запросы субъектов персональных данных		
12.7	Соблюдение условий и порядка обработки персональных данных граждан, обратившихся в министерство		
12.8	Соблюдение процедур, направленных на предотвращение и выявление нарушений законодательства РФ в сфере персональных данных		
13	**Нормативно-методическое обеспечение системы защиты информации**		
13.1	Проверка наличия модели угроз безопасности информации и степени ее актуальности с учетом используемых технологий обработки информации (срок актуальности документа не может превышать 3 лет)		
13.2	Проверка наличия Эскизного проекта системы обеспечения информационной безопасности		

1	2	3	4
13.3	Проверка ознакомления работников с нормативными документами, регламентирующими процессы обработки и защиты информации (в том числе персональных данных)		Может проводиться в формате тестирования или анкетирования с установленным перечнем контрольных вопросов

Дата _____20__ г.

Составитель _____ Ф.И.О.
(подпись)

Приложение 2
к политике аудита
информационной безопасности
министерства образования,
науки и молодежной политики
Краснодарского края

ФОРМА ПЛАНА
проведения периодического внутреннего аналитического
аудита информационной безопасности

(наименование структурного подразделения)

государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий»

№ п/п	Объекты проверки	Результаты проверки	Примечание
1	2	3	4
1.1	Проверка перечня используемых для доступа к АРМ учетных записей пользователей с фактическими, использованными для доступа к АРМ		
1.2	Проверка на АРМ пользователей информации (в том числе в истории Интернет-браузеров), не относящейся к служебным обязанностям		
1.3	Проверка состава, используемого на АРМ пользователей программного обеспечения (в соответствии с Реестром разрешенного к использованию ПО)		
1.4	Проверка наличия печатей (пломб) на АРМ		
1.5	Проверка наличия установленных на АРМ паролей на доступ к BIOS		
1.6	Проверка возможности использования на АРМ пользователей технологий беспроводной передачи данных, веб-камер и микрофонов		
1.7	Проверка работоспособности на АРМ и серверах средств защиты информации		
1.8	Проверка настроек программного обеспечения и средств защиты информации требованиям эксплуатационной документации		Проверяется в том числе актуальность антивирусных баз

1	2	3	4
1.9	Проверка АРМ и серверов на предмет подключения к ним мобильных устройств передачи информации (в ретроспективе), а также неучтенных съемных носителей информации		
2	**Учет и использование съемных носителей информации**		
1.2	Проверка наличия перечня мест хранения съемных носителей, назначения ответственных за них лиц и степени их актуальности		
2.2	Проверка съемных носителей информации на предмет наличия информации, не связанной с использованием служебных обязанностей		
1.3	Проверка выполнения уничтожения (стирания) информации со съемных носителей информации		
2.3	Проверка выполнения порядка уничтожения съемных носителей информации		
3	**Использование аутентификационной информации при доступе к информационным активам**		
3.1	Выборочная проверка реализации требований, установленных к качеству аутентификационной информации и мер по обеспечению ее безопасности		После проверок исполнения требований к качеству пароля (приводящие к его санкционированной компрометации), пользователь должен продемонстрировать установленный пароль на доступ, после чего незамедлительно его сменить
3.2	Отсутствие сохраненных паролей доступа как средствами программного обеспечения, так и на бумажных носителях (вне отведенных для этого местах)		
4	**Организация доступа в помещения обработки информации и выполнение требований, установленных к таким помещениям**		
4.1	Проверка наличия перечня лиц, допущенных в помещения обработки конфиденциальной информации, степени его актуальности		Проверка наличия перечня для каждого помещения, а также в ходе проведения аудита - проверяется степени исполнения данного требования при доступе в помещения
4.2	Проверка наличия перечня мест хранения материальных носителей персональных данных и ответственных, степени актуальности данного перечня		
5	**Учет и использование средств криптографической защиты информации**		
5.1	Проверка условий эксплуатации СКЗИ, в том числе выполнение требований		

1	2	3	4
	эксплуатационной документации на СКЗИ		
5.2	Проверка ознакомления работников с нормативными документами, регламентирующими процессы обработки и защиты информации (в том числе персональных данных)		Может проводить в формате тестирования или анкетирования с установленным перечнем контрольных вопросов

Дата _____20__ г.

Составитель _____ Ф.И.О.
(подпись)

Приложение 3
к политике аудита
информационной
безопасности министерства
образования, науки и
молодежной политики
Краснодарского края

ФОРМА ПЛАНА
устранения недостатков, выявленных в ходе проведения внутреннего аналитического аудита информационной безопасности

№ п/п	Нарушение / недостаток	Мероприятия по устранению	Срок исполнения	Ответственные за исполнение
1	2	3	4	5

Дата _____20__ г.

Составитель _____ Ф.И.О.
(подпись)