ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Ухтинский техникум железнодорожного транспорта – филиал федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Петербургский государственный университет путей сообщения Императора Александра I» (УТЖТ – филиал ПГУПС)

УТВЕРЖДАЮ:
Директор
_____В.Г. Бестужев
31 12 .2014

Приложение
к приказу от 31.12.2014
№ 1075

СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

ПОЛОЖЕНИЕ

О ПОЛИТИКЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УТЖТ - ФИЛИАЛА ПГУПС

УФ СМК РД 6.6.04-2014

Экз № 1

Копия №_____

Ухта
2014

ПРЕДИСЛОВИЕ

1. РАЗРАБОТАНО начальником информационно-вычислительного центра
2. ВВЕДЕНО взамен Положения о Политике информационной безопасности УТЖТ-филиала ПГУПС, утвержденного приказом директора №828 от 09.11.2011;
3. ПРИНЯТО решением Совета УТЖТ – филиала ПГУПС, протокол № 91 от 26.12.2014.
4. УТВЕРЖДЕНО директором УТЖТ – филиала ПГУПС 31.12.2014.
5. Периодичность проверки 5 лет.

Содержание

1. Область применения

Настоящее Положение регламентирует вопросы управления информационной безопасностью, планирование, реализацию и поддержку решений безопасности в УТЖТ-филиале ПГУПС.

Настоящее Положение входит в состав документов системы менеджмента качества.

2. Нормативные ссылки

В настоящем Положении использованы ссылки на следующие нормативные документы:

ISO 9000:2005 Системы менеджмента качества. Основные положения и словарь.

ISO 9001:2008 Системы менеджмента качества. Требования.

СМК ДП 4.2.03-2013 Система менеджмента качества. Документированная процедура. Общие требования к построению, изложению и оформлению документации системы менеджмента качества.

СМК ДП 4.2.01-2013 Система менеджмента качества. Документированная процедура. Управление документацией.

СМК ДП 4.2.04-2013 Система менеджмента качества. Документированная процедура. Нормоконтроль документации системы менеджмента качества.

СМК МИ 3.1.01-2011 Система менеджмента качества. Методическая инструкция. Термины и определения в области управления качеством в области высшего и среднего профессионального образования.

Доктрина информационной безопасности Российской Федерации утв. Президентом РФ от 09.09.2000г. № Пр-1895;

Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации».

Федеральный закон “Об информации, информационных технологиях и о защите информации” от 27.07.2006 № 149-ФЗ;

Федеральный закон “О персональных данных” от 27.07.2006 № 152-ФЗ;

Федеральный закон “О коммерческой тайне” от 29.07.2004 № 98 – ФЗ;

ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью.

Устав Университета

Положение об УТЖТ – филиале ПГУПС.

3. Термины и определения

В настоящем Положении применяются термины и определения в соответствии с ISO 9000 и СМК МИ 3.1.01., а также в соответствии с ГОСТ Р 50922-2006 Защита информации. Основные термины и определения; Рекомендациями по стандартизации Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации; Рекомендациями по стандартизации Р 50.1.056 – 2005 Техническая защита информации. Основные термины и определения.

Термин	Определение
Авторизация (санкционирование доступа)	предоставление субъекту права на доступ, а также предоставление доступа в соответствии с установленными правами на доступ
Автоматизированная система	система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций
Аудит информационной безопасности	Периодический, независимый и документированный процесс получения свидетельств аудита и их оценки с целью установления степени выполнения установленных требований по обеспечению информационной безопасности
Аутентификация	действия по проверке подлинности субъекта доступа в информационной системе
Безопасность информации	состояние защищенности информации, при котором обеспечиваются такие ее характеристики, как конфиденциальность, целостность и доступность. Определяется отсутствием недопустимого риска
Безопасность информационной технологии	состояние защищенности информационной технологии, при котором реализуется выполнение предписанных функций без нарушений безопасности информации
Доступность	состояние, при котором субъекты, имеющие права доступа могут реализовать их беспрепятственно
Жизненный цикл	совокупность взаимосвязанных процессов создания и последовательного изменения состояния объекта от формирования исходных требований к нему до утилизации
Защищаемая информация	информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов, либо требованиями, устанавливаемыми собственником информации
Идентификация	действия по предоставлению субъектам и объектам доступа идентификаторов и (или) предоставление доступа путем сравнения предъявляемого идентификатора с перечнем присвоенных идентификаторов

Информация	сведения (сообщения, данные) независимо от формы их представления
Информационная система	организационно упорядоченная совокупность операторов, документов и информационных технологий, в том числе с использованием средств вычислительной техники и связи
Информационные активы	технические, программные и программно – аппаратные комплексы, а также информация (служебная, управляющая, финансовая, аналитическая и т.д.) обрабатываемая ими во всех фазах жизненного цикла (создание, обработка, хранение, распространение, уничтожение);
Инцидент, относящийся к информационной безопасности	единичное событие, либо ряд нежелательных или непредвиденных событий, относящихся к информационной безопасности (события безопасности), влекущих существенную вероятность нарушения информационной безопасности информационных активов
Компрометация конфиденциальности информации	несанкционированное получение, разглашение, информации, либо передача её третьим лицам без согласия ее обладателя
Конфиденциальность	состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на это право
Криптографическая защита	Защита информации при помощи криптографического преобразования данных
Критичная информация	информация, компрометация конфиденциальности которой оказывает негативное влияние на функционирование информационных систем, приводит к причинению материального или иного вида ущерба
Мониторинг безопасности информации	постоянное наблюдение за процессом обеспечения безопасности информации в информационной системе с целью выявления его соответствия требованиям по безопасности информации
Несанкционированное воздействие	изменение информации, осуществляемое с нарушением установленных прав и (или) правил

Несанкционированный доступ	доступ к информации, осуществляемый с нарушением установленных прав и (или) правил разграничения доступа к информации
Оценка (анализ) рисков	выявление угроз безопасности информации, уязвимостей информационных систем, оценка вероятностей реализации угроз с использованием уязвимостей и их последствий для информации и информационной системы, используемой для ее обработки
Пользователь информационной системы	Субъект, в установленном порядке получивший права на доступ к ресурсам информационной системы, в соответствии со своими функциональными обязанностями
Профиль защиты	совокупность типовых требований по обеспечению безопасности информации, которые должны быть реализованы в защищаемой информационной системе
Регистрационная (учетная) запись пользователя	совокупность сведений о субъекте доступа, включающая в себя его уникальный идентификатор, однозначно идентифицирующий данного пользователя в информационной системе
Риск	совокупность вероятностей возникновения ущерба вследствие реализации объективных и субъективных, внешних и внутренних, случайных и преднамеренных угроз, оказывающих влияние на функционирование информационных систем с учетом величины ущерба
Система обеспечения информационной безопасности (СОИБ)	система организационно-технических мероприятий, основной целью создания и функционирования которой является обеспечение защиты информации Техникума путем внедрения и эксплуатации технических систем, комплексов и средств информационной безопасности, обеспечивающих доступность соответствующих категорий информации для обучающихся и работников Техникума, других организаций и частных лиц; управление информационной безопасностью Техникума и ее аудит
Средства обеспечения информационной безопасности	Организационные, технические, программные или программно – аппаратные средства, используемые для обеспечения защиты информации на всех стадиях жизненного цикла защищаемого объекта

Техническая защита информации	обеспечение безопасности информации, подлежащей защите в соответствии с действующим законодательством с применением технических, программных и программно – аппаратных средств
Угроза	совокупность условий и факторов, определяющих потенциальную или реально существующую опасность нарушения безопасности информации
Утечка информации	неконтролируемое распространение защищаемой информации
Физическая защита информации	обеспечение безопасности информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты
Целостность	состояние информации, при котором ее изменение осуществляется только преднамеренно субъектами, имеющими на него право

4. Обозначения и сокращения

В настоящем Положении применяются следующие сокращения

Техникум — Ухтинский техникум железнодорожного транспорта – филиал федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Петербургский государственный университет путей сообщения Императора Александра I» (УТЖТ – филиал ПГУПС);

СМК - система менеджмента качества;

Обучающийся - физическое лицо, осваивающее образовательную программу.

Студент – это лицо, осваивающее образовательные программы среднего профессионального, программы бакалавриата, программы специалитета или программы магистратуры. (Федеральный закон от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации»).

АС	–	автоматизированная система
АРМ	–	автоматизированное рабочее место
ИБ	–	информационная безопасность
ИВЦ	–	информационно-вычислительный центр – структурное подразделение Техникума
ИОК	–	инфраструктура открытых ключей
КИ	–	конфиденциальная информация

НДВ	–	недекларированные возможности
НСВ	–	несанкционированное воздействие
НСД	–	несанкционированный доступ
ОПД	–	ответственные за персональные данные в структурном подразделении
ПЗ	–	профиль защиты
ПДТК	–	постоянно действующая техническая комиссия
ПО	–	программное обеспечение
СЗИ	–	средство защиты информации
СПД	–	сеть передачи данных
СОИБ	–	система обеспечения информационной безопасности
СПТ	–	структурное подразделение Техникума
СУИБ	–	система управления информационной безопасностью
ТЗИ	–	техническая защита информации

5. Ответственность и полномочия

5.1. Настоящее Положение принимается решением Совета Техникума и утверждается директором Техникума.

5.2. Ответственность за реализацию данного Положения несет начальник ИВЦ.

6. Общие положения

6.1. Настоящая Политика информационной безопасности направлена на достижение главных целей обеспечения информационной безопасности Техникума:

- обеспечение приемлемого уровня рисков экономического и иных видов ущерба при нарушении безопасности информации;
- поддержание высокого уровня безопасности информации обрабатываемой и накапливаемой в Техникуме в условиях автоматизации процессов обучения, исследовательских и иных работ, направленных на достижение целей, оговоренных Уставом;
- обеспечение своевременного и надежного доступа к соответствующим категориям информации обучающихся, работников Техникума, других организаций и частных лиц.

6.2. Настоящая Политика определяет:

- основные цели, задачи, общие принципы и направления обеспечения информационной безопасности в структурных подразделениях;
- порядок осуществления и контроля выполнения в Техникуме положений Федерального законодательства РФ в области защиты информации;
- ответственность работников Техникума и пользователей его информационных систем за нарушение требований, устанавливаемых настоящей Политикой.

6.3. Под Политикой информационной безопасности Техникума (далее - Политика) понимается совокупность документированных управленческих и организационно – технических решений, направленных на обеспечение необходимого уровня безопасности информации, обрабатываемой в Техникуме.

6.4. Требования настоящего Положения распространяются на все структурные подразделения Техникума.

6.5. Требования настоящей Политики распространяются на обеспечение информационной безопасности конфиденциальной информации в Техникуме.

6.6. Основными целями Политики информационной безопасности являются:

- предотвращение НСД к конфиденциальной информации Техникума, в том числе обрабатываемой в АС;
- обеспечение целостности и доступности информации Техникума;
- защита от незаконного вмешательства в процесс обработки информации Техникума, в том числе в функционирование его АС;
- защита от НСД к информационным активам Техникума, в том числе в его АС;
- анализ рисков информационной безопасности Техникума;
- обеспечение ответственности работников и обучающихся Техникума при работе с внутренними и внешними информационными системами, ресурсами и активами.

6.7. Основными задачами обеспечения информационной безопасности Техникума являются:

- определение информационных активов, подлежащих защите;
- категорирование информационных активов и классификация информационных систем Техникума в соответствии с приоритетами и требуемым уровнем защиты информации;
- анализ уязвимостей, прогнозирование и выявление внутренних и внешних угроз информационной безопасности Техникума, оценка защищенности активов;
- определение необходимых параметров, характеризующих величину рисков информационной безопасности;
- защита от несанкционированного вмешательства в процесс обработки информации Техникума, в том числе в АС;
- разграничение ответственности между подразделениями Техникума, отвечающими за процессы обработки информации и подразделениями Техникума, осуществляющими защиту информационных активов;
- наделение полномочиями подразделений Техникума реализующих информационную безопасность;
- поддержание в актуальном состоянии документального обеспечения подразделений, осуществляющих защиту информационных активов Техникума;
- защита от несанкционированного доступа к конфиденциальной информации, обрабатываемой Техникумом и передаваемой по телекоммуникационным каналам связи;

- обеспечение целостности общесистемного и прикладного программного обеспечения АС Техникума, в рамках полномочий структурных подразделений Техникума, восстановление их целостности в случае нарушения;
- защита от воздействия вредоносного программного обеспечения;
- обеспечение защиты информации при использовании общедоступных телекоммуникационных сетей передачи данных (в том числе сети Internet);
- защита от утечки по техническим каналам конфиденциальной информации Техникума, в том числе хранимой и обрабатываемой в АС и передаваемой по телекоммуникационным каналам связи;
- аудит информационных активов, вычислительных средств и сетевых информационных ресурсов Техникума;
- физическая защита объектов, оборудования, производственных и служебных помещений Техникума, относящихся к категории информационных активов.

6.8. Информационная безопасность Техникума обеспечивается:

- определением допустимого ущерба;
- минимизацией рисков нанесения ущерба в условиях действия объективных и субъективных, внешних и внутренних, случайных и преднамеренных угроз.

6.9. Работники, нарушающие требования настоящей Политики, несут дисциплинарную, гражданско-правовую, административную и уголовную ответственность в соответствии с действующим законодательством Российской Федерации.

7. Организационная структура и нормативно-методическое обеспечение информационной безопасности Техникума, разграничение полномочий и ответственности в процессе обработки информации

7.1. Ответственность за реализацию и соблюдение требований настоящей Политики возлагается:

- на руководителей структурных подразделений Техникума.

7.2. К подразделениям, отвечающим за обеспечение информационной безопасности Техникума, относятся:

- информационно-вычислительный центр;
- структурные подразделения, в части их касающейся;

7.3. Подразделения защиты информации Техникума обеспечивают:

7.3.1. Информационно-вычислительный центр:

7.3.1.1. Начальник ИВЦ:

- назначение и контроль прав доступа пользователей к АС Техникума, сопровождаемым информационным системам;
- организация централизованных закупок программных и программно – аппаратных средств обеспечения информационной безопасности Техникума;
- организацию обучения авторизованных пользователей информационных систем Техникума;
- организацию сдачи-приемки в эксплуатацию информационных систем и СОИБ, в части их касающейся;

- разработка инструкций и иной распорядительной документации по вопросам эксплуатации информационных систем, телекоммуникационных каналов связи в части их касающейся
- определение параметров, характеризующих величину рисков ИБ;
- организацию обеспечения и контроль выполнения требований по ИБ в структурных подразделениях Техникума в области технической защиты информации, в области криптографической защиты информации (в части защиты персональных данных);
- организацию мониторинга ИБ Техникума, в том числе в информационных системах, функционирующих в других структурных подразделениях;
- организацию контроля выполнения требований лицензирующих органов в части выполнения требований по защите информации, не составляющую государственную тайну;
- организация снабжения Техникума программными продуктами контроля защищенности информации;
- оказание методической помощи по вопросам ИБ структурным подразделениям Техникума;
- организацию консультирования пользователей различного уровня по вопросам эксплуатации и применения средств защиты и контроля информации;
- организацию устранения выявленных уязвимостей и нарушений ИБ;
- статистическую обработку данных по фактам нарушения ИБ для определения параметров рисков ИБ;
- проведение лицензионной работы в области информационной безопасности;
- подготовку и представление ПДТК и администрации Техникума предложений по совершенствованию функционирования СОИБ;
- представление отчетности по ИБ.

7.3.1.2. Системный администратор

- координацию мероприятий по информационной безопасности;
- настройку систем обеспечения ИБ эксплуатируемых систем в соответствии с требованиями ИБ, организационно – распорядительной и эксплуатационной документацией;
- администрирование эксплуатируемых СОИБ;
- разработку инструкций и другой организационно-распорядительной документации по вопросам эксплуатации СОИБ в сфере своей ответственности;
- эксплуатацию СОИБ в соответствии с эксплуатационной документацией;
- условия проведения мониторинга и мониторинг ИБ;
- устранение выявленных уязвимостей и нарушений ИБ;
- подготовку предложений по финансированию мероприятий, связанных с обеспечением ИБ;
- подготовку предложений и рекомендаций по совершенствованию СОИБ и представление этих предложений в службу технической защиты информации Техникума;
- подготовку отчетных материалов по результатам работы средств защиты информации и нарушениям ИБ и представление их в службу технической защиты информации Техникума;

- организацию консультирования и инструктажа пользователей различного уровня по вопросам эксплуатации применяемых средств защиты и контроля в пределах зон ведения.

7.3.2. Структурные подразделения, в части их касающейся:

- выполнение положений настоящей Политики безопасности;
- выполнение требований ИВЦ;
- выполнение регламентов по технической защите информации;
- эксплуатацию средств обеспечения информационной безопасности информационных систем Техникума в пределах зоны ведения;
- разработку и согласование инструкций и другой организационно-распорядительной документации по вопросам обеспечения ИБ Техникума в сфере своей ответственности;
- эксплуатацию АС Техникума и СОИБ в соответствии с эксплуатационной документацией;
- подготовку предложений и рекомендаций по совершенствованию СОИБ и представление этих предложений в ИВЦ.

8. Основные информационные активы Техникума, подлежащие защите, их категорирование

8.1. Информационные активы Техникума включают материальные носители, технические, программные и программно-технические средства, используемые для накопления, хранения, обработки, передачи и защиты информации.

8.2. Основными информационными активами (ресурсами) Техникума, подлежащими защите, являются:

- конфиденциальная информация, определенная законодательством РФ и распорядительной документацией Техникума
- персональные данные работников Техникума, обучающихся в нём и других физических лиц;
- информация, составляющая коммерческую тайну Техникума и третьих лиц;
- информация, составляющая интеллектуальную собственность Техникума и третьих лиц;
- служебная информация, в том числе средств защиты информации (идентификаторы, пароли, таблицы разграничения доступа, криптографические ключи, информация журналов аудита безопасности и др.);
- программно-аппаратные комплексы АС;
- программно-аппаратные комплексы систем защиты информации;
- программно-аппаратные комплексы информационных систем и баз данных.

8.3. Категорирование информационных активов выполняется в соответствии с нормативно – руководящими документами и утвержденными методиками.

8.4. Информационные активы, подлежащие защите, уточняются по результатам категорирования и оформляются в виде Перечня защищаемых активов, утверждаемого установленным в Техникуме порядком.

8.5. Информационные ресурсы (активы) должны быть защищены средствами защиты информации в соответствии с установленной категорией и нормативно – руководящими документами.

9. Основные угрозы информационным активам Техникума

9.1. Основными угрозами информационным активам Техникума, являются:

- разглашение (утечка) защищаемой информации Техникума;
- несанкционированный доступ к информационным активам Техникума;
- несанкционированное воздействие на информационные активы Техникума;
- нарушение целостности информационных активов Техникума, включая изменение или фальсификацию (искажение и модификацию), а также полное или частичное уничтожение информации;
- дезорганизация функционирования информационных активов Техникума;
- недостатки организационного обеспечения защиты информации.

10. Методы реализации Политики информационной безопасности

Цели настоящей Политики информационной безопасности Техникума по защите его информационных активов достигаются обеспечением:

10.1. Разграничения доступа пользователей к информационным системам Техникума и регистрации их действий

10.2. Защиты процессов функционирования информационных систем Техникума от несанкционированного вмешательства

10.3. Защиты информационных систем Техникума при использовании внутренних и внешних телекоммуникационных сетей

10.4. Защиты информационных систем Техникума от воздействий вредоносного программного обеспечения

10.5. Защиты от несанкционированного доступа к информации, обрабатываемой в информационных системах Техникума и передаваемой по телекоммуникационным каналам

10.6. Защиты информации, являющейся конфиденциальной, от утечки по техническим каналам

10.7. Защиты физическими и организационно-техническими методами материальных составляющих информационных систем и активов Техникума

10.8. Контроля состояния защищенности информационных систем Техникума

Методология реализации Политики информационной безопасности приведена в Положении об обеспечении информационной безопасности в информационной системе УТЖТ-филиала ПГУПС.docx.

11. Контроль выполнения требований Политики информационной безопасности Техникума

11.1. Контроль выполнения требований настоящей Политики осуществляется подразделениями, отвечающими за обеспечение информационной безопасности Техникума:

- информационно-вычислительный центр;
- структурными подразделениями, в части их касающейся.

11.2. Контроль степени выполнения установленных Политикой информационной безопасности Техникума требований осуществляется проведением аудита:

- внутреннего аудита;
- внешнего аудита.

12. Согласование, хранение, рассылка и изменения

12.1. Согласование настоящего Положения осуществляется с заместителем директора по АХЧ, безопасности, учебной, учебно-производственной, воспитательной работе, главным бухгалтером, начальником ИВЦ, начальником отдела кадров, заведующими отделениями, ведущим юрисконсультом, лицом, осуществляющим нормоконтроль, и оформляется в «Листе согласования».

12.2. Нормоконтроль настоящего Положения осуществляется в соответствии с СМК ДП 4.2.04.

12.3. Ответственность за хранение подлинника возлагается на заместителя директора по учебной работе, ответственность за тиражирование на начальника ИВЦ, ответственность за рассылку учтенных рабочих экземпляров абонентам возлагается на инспектора (приемная директора).

12.4. Рассылка учтенных рабочих экземпляров осуществляется: заместителям директора по АХЧ, безопасности, учебной, учебно-производственной, воспитательной работе, главному бухгалтеру, начальнику ИВЦ, начальнику отдела кадров, заведующим отделениям.

12.5. Выдача учтенных рабочих экземпляров регистрируется согласно СМК ДП 4.2.01.

12.6. Изменения настоящего Положения должно производиться в соответствии с СМК ДП 4.2.01 и оформляться в Листе регистрации изменений.

Лист согласования

Должность	ФИО	Дата	Подпись
Заместитель директора по учебной работе	Т.М. Коротаева	26.12.14	
Заместитель директора по учебно-производственной работе	Н.И. Прокопович	26.12.14	
Заместитель директора по воспитательной работе	И.И.Хаменева	26.12.14	
Заместитель директора по АХЧ	В.А.Моисеев	26.12.14	
Заведующий очным отделением	П.Е. Меграбян	26.12.14	
Заведующий очным отделением	И.П. Балеева	26.12.14	
Заведующий заочным отделением	А.М. Талебина	26.12.14	
Главный бухгалтер	Т.П. Куткина	26 12 14	
Начальник отдела кадров	Е.Н.Кузьбожева	26.12.14	
Начальник ИВЦ	Ю.Б.Колосовский	26.12.14	
Ведущий юрисконсульт	И.В.Фадеева	26.12.14	
Нормоконтроль	Т.М. Коротаева	26.12.14	

Лист ознакомления

Должность	ФИО	Дата	Подпись
Заместитель директора по учебной работе	Т.М. Коротаева	31.12.14	
Заместитель директора по учебно-производственной работе	Н.И. Прокопович	31.12.14	
Заместитель директора по воспитательной работе	И.И.Хаменева	31.12.14	
Заместитель директора по АХЧ	В.А.Моисеев	31.12.14	
Заведующий очным отделением	П.Е. Меграбян	31.12.14	
Заведующий очным отделением	И.П. Балеева	31.12.2014	
Заведующий заочным отделением	А.М. Талебина	31.12.2014	
Главный бухгалтер	Т.П. Куткина	31.12.2014	
Начальник отдела кадров	Е.Н.Кузьбожева	31.12.14	
Начальник ИВЦ	Ю.Б.Колосовский	31.12.14	

Лист регистрации изменений

Номер изменения	Номер извещения об изменении	Номер листов (страниц)				Всего листов (после изменений)	Дата внесения	ФИО, осуществляющего внесение изменений	Подпись, вносившего изменения
		Измененных	Замененных	Новых	Аннулированных				

Лист учета периодических проверок

Дата проверки	ФИО лица, выполнившего проверку	Подпись выполнившего проверку	Формулировки замечаний