ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ
ЧАСТНОЕ УЧРЕЖДЕНИЕ
«ЮРИДИЧЕСКИЙ ТЕХНИКУМ» Г. КРОПОТКИН

ОДОБРЕНО

Решением Педагогического Совета
от 29 августа 2016 года
№1

УТВЕРЖДЕНО
Приказом от 29.08.2016 г. № 1-У

Директор _____ Е.А. Савина

Рег. № 018
от «01» сентября 2016 г.

ПОЛОЖЕНИЕ
ПО ОРГАНИЗАЦИИ И ПРОВЕДЕНИЮ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

в Профессиональной образовательной организации
частном учреждении «Юридический техникум» г. Кропоткин

Кропоткин
2016

1. Общие положения

1.1 Настоящее Положение разработано с целью определения содержания и порядка осуществления мероприятий по защите персональных данных (далее – ПДн), обрабатываемых в информационных системах персональных данных (далее – ИСПДн) ПОО ЧУ «Юридический техникум» г. Кропоткин (далее – оператор).

Систему защиты персональных составляют документы:

- Постановление Правительства «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01 ноября 2012г. №1119;
- «Порядок проведения классификации информационных систем персональных данных», утвержденный совместным приказом ФСТЭК России, ФСБ России, Министерства информационных технологий и связи Российской Федерации от 13 февраля 2008 г. № 55/86/20 (зарегистрирован в Минюсте Российской Федерации 03.04.2008 № 11462);
- Приказ №58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных», утвержденный 05 февраля 2010 г. директором ФСТЭК России;
- «Базовая модель угроз безопасности персональных данных при обработке в информационных системах персональных данных», утверждена 15 февраля 2008г. заместителем директора ФСТЭК России;
- «Методика определения актуальных угроз безопасности персональных данных при обработке в информационных системах персональных данных», утверждена 14 февраля 2008 г. заместителем директора ФСТЭК России.

2. Состав персональных данных в ИСПДн оператора

Персональные данные граждан, циркулирующие в информационной системе персональных данных накапливаются и обрабатываются в процессе деятельности оператора.

Перечень защищаемых персональных данных, обрабатываемых в ИСПДн оператора, определяется документом «Перечень персональных данных, подлежащих защите», утверждаемым приказом руководителя.

3. Основные условия проведения обработки персональных данных

3.1 Обработка персональных данных осуществляется:

- после получения согласия субъекта персональных данных, за исключением случаев, предусмотренных частью 2 статьи 6 Федерального закона;
- после принятия необходимых мер по защите персональных данных.

3.2 В ПОО ЧУ «Юридический техникум» г. Кропоткин приказом руководителя назначается сотрудник, ответственный за защиту персональных данных, и определяется перечень лиц, допущенных к обработке персональных данных.

4. Порядок обработки персональных данных в информационных системах персональных данных с использованием средств автоматизации

4.1 Обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации осуществляется в соответствии с требованиями постановления Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», нормативных и руководящих документов уполномоченных федеральных органов исполнительной власти.

4.2 Не допускается обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации:

- при отсутствии установленных и настроенных сертифицированных средств защиты информации;

- при отсутствии утвержденных организационных документов о порядке эксплуатации информационной системы персональных данных.

5. Порядок обработки персональных данных без использования средств автоматизации

5.1 Обработка персональных данных без использования средств автоматизации (далее – неавтоматизированная обработка персональных данных) может осуществляться в виде документов на бумажных носителях.

5.2 При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

5.3 При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;

- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

5.4 При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовые формы), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, - при необходимости получения письменного согласия на обработку персональных данных;

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы;

5.5 Необходимо принимать организационные (охрана помещений) и технические меры, исключающие возможность несанкционированного доступа к материальным носителям персональных данных лиц, не допущенных к их обработке;

5.6 При несовместимости целей неавтоматизированной обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

б) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием

сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

5.7 Документы, содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

Уничтожение или обезличивание части персональных данных может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

6. Организационные и технические мероприятия по защите персональных данных

Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

а) определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

б) разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

в) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

г) установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

д) обучение лиц, использующих средства защиты информацию, применяемые в информационных системах, правилам работы с ними;

е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

ж) учет лиц, допущенных к работе с персональными данными в информационной системе;

з) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

к) описание системы защиты персональных данных.

7. Обязанности должностных лиц

Ответственность за организацию работ по защите персональных данных возлагается на системного администратора.

Для непосредственного выполнения мероприятий по защите персональных данных или осуществления взаимодействия с организациями лицензиатами, привлекаемыми для выполнения работ по защите персональных данных, назначается сотрудник, обладающий необходимыми знаниями в данной области.

Всем сотрудникам, привлекаемым для работы с персональными данными, в обязательном порядке, под роспись доводятся правила и требования по работе со средствами защиты информации. Не реже, чем раз в полгода сотрудником, отвечающим за выполнение мероприятий по защите информации, должны проводиться проверки правильности эксплуатации средств защиты.

8. Контроль состояния защиты персональных данных

В информационных системах персональных данных все обращения на получение персональных данных и результаты таких обращений должны регистрироваться автоматизированными средствами информационной системы в электронном журнале обращений.

При обработке персональных данных в ИСПДн должно быть обеспечено:

а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

б) своевременное обнаружение фактов несанкционированного доступа к персональным данным;

в) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

г) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

д) постоянный контроль за обеспечением уровня защищенности персональных данных.

При обнаружении нарушений порядка предоставления персональных данных сотрудник, ответственный за организацию работ по защите персональных данных, обрабатываемых оператором, незамедлительно приостанавливает предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

Достаточность принятых мер по обеспечению безопасности персональных данных при их обработке в информационных системах оценивается при проведении государственного контроля и надзора.

9. Аттестация информационной системы персональных данных

Аттестация информационной системы по требованиям безопасности информации проводится организацией, имеющей лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации, в соответствии со схемой, выбираемой организацией-лицензиатом на этапе подготовки к аттестации.

В общем виде аттестация ИСПДн по требованиям безопасности информации включает в себя следующие этапы:

- анализ исходных данных по аттестуемой ИСПДн;
- предварительное ознакомление с аттестуемой ИСПДн;
- проведение экспертного обследования ИСПДн и анализ разработанной документации по обеспечению безопасности ПДн на соответствие требованиям нормативных и методических документов;
- проведение комплексных аттестационных испытаний ИСПДн в реальных условиях эксплуатации с использованием специальной аппаратуры контроля и программных средств контроля защищенности от несанкционированного доступа;
- анализ результатов комплексных аттестационных испытаний, оформление и утверждение заключения по результатам аттестации.

Приложения:

1. Правила парольной защиты (Приложение 1).
2. Правила антивирусной защиты (Приложение 2).
3. Правила обновления общесистемного и прикладного программного обеспечения ИСПДн (Приложение 3).
4. Порядок работы с электронным журналом обращений пользователей информационной системы к ПДн (Приложение 4).

5. Порядок предоставления информации органам государственной власти и местного самоуправления, физическим и юридическим лицам (Приложение 5).
6. Порядок проведения служебного расследования нарушений режима информационной безопасности ИСПДн (Приложение 6).
7. Порядок приостановки предоставления ПДн в случае обнаружения нарушений порядка их обработки (Приложение 7).
8. Инструкция по организации резервирования и восстановления программного обеспечения, баз персональных данных информационных систем персональных данных (Приложение 8).

Приложение 1

Правила парольной защиты

1. Общие положения

Целью применения и реализации Правил парольной защиты является недопущение утечки ПДн, а также их несанкционированной модификации или уничтожения и действует для всех пользователей и администраторов ИСПДн оператора.

Правила парольной защиты регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в ИСПДн, а также контроль над действиями пользователей при работе с паролями.

Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями пользователей при работе с паролями возлагается на администратора безопасности.

Личные пароли должны генерироваться и распределяться централизованно либо создаваться пользователями ИСПДн самостоятельно с учетом следующих требований:

- пароль должен быть не менее 6-ти символов;
- в числе символов пароля ***обязательно должны присутствовать*** буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от значений 24-х предыдущих паролей;
- максимальный срок действия пароля пользователя составляет 90 дней;
- минимальный срок действия пароля пользователя составляет 2 дня;
- пользователь не имеет права сообщать личный пароль другим лицам.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

При наличии, в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п., технологической необходимости использования имен и паролей сотрудников (исполнителей) в их отсутствие, сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте или опечатанном пенале передавать на хранение администратору безопасности. Опечатанные конверты (пеналы) с паролями исполнителей должны храниться в сейфе.

Полная плановая смена паролей пользователей должна проводиться регулярно, не реже двух раз в квартал.

Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу внутри предприятия и т.п.) должна производиться немедленно после окончания последнего сеанса работы данного пользователя с системой на основании письменного указания начальника отдела.

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри предприятия и другие обстоятельства) администратора безопасности.

2. Контроль

Контроль за действиями пользователей ИСПДн при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на администратора безопасности.

Приложение 2

Правила антивирусной защиты

1. Общие требования

Правила антивирусной защиты определяют требования к организации защиты ИСПДн от разрушающего воздействия вредоносных программ и устанавливают ответственность руководителя и сотрудников, эксплуатирующих и сопровождающих ИСПДн, за их выполнение.

Целью защиты ИСПДн от вредоносных программ является предотвращение и нейтрализация негативных воздействий вредоносных программ на средства вычислительной техники.

К использованию в ИСПДн допускаются только лицензионные и сертифицированные ФСТЭК или ФСБ России по требованиям безопасности информации средства защиты от вредоносных программ.

Установка и начальная настройка средств защиты от вредоносный программ в ИСПДн осуществляется представителями организации – лицензиата ФСТЭК России, впоследствии – администратором безопасности.

Администратор безопасности должен организовывать осуществление периодического обновления сигнатур средств защиты от вредоносных программ и контроль их работоспособности не реже чем один раз в неделю.

Пользователи ИСПДн обязаны руководствоваться в работе настоящими правилами антивирусной защиты и «Инструкцией пользователя ИСПДн...».

2. Применение средств защиты от вредоносных программ

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль.

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.

В ИСПДн запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь самостоятельно (или вместе с администратором безопасности, если он назначен на объекте) должен провести внеочередной антивирусный контроль своего персонального компьютера.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить работу персонального компьютера;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности;
- провести «лечение» или удаление зараженных файлов.

3. Ответственность

Ответственность за организацию антивирусного контроля в ИСПДн в соответствии с требованиями Настоящих Правил возлагается на администратора безопасности.

Ответственность за проведение мероприятий антивирусной защиты ИСПДн и соблюдение требований Настоящих Правил возлагается на администратора безопасности и всех пользователей ИСПДн.

Приложение 3

Правила обновления общесистемного и прикладного программного обеспечения ИСПДн

1. Общие положения

В системе управления ИСПДн оператора должна обеспечиваться и регламентироваться деятельность, связанная с установкой нового оборудования, либо его компонентов, патчей, а также обновлений операционных систем (далее – ОС) и других приложений.

Тестирование нового оборудования и обновлений программного обеспечения (далее – ПО) не должно осуществляться на ресурсах действующей информационной инфраструктуры.

Правила и порядок обновления ПО, ОС и приложений в целях информационной безопасности ИСПДн направлены на защиту ресурсов от:

- нарушения штатной работы информационных ресурсов и сервисов;
- разрушения;
- нарушения штатного функционирования оборудования;
- несанкционированной модификации;
- несанкционированного копирования.

2. Правила управления обновлениями ПО ИСПДн в информационной инфраструктуре оператора.

- Отслеживание появления новых уязвимостей в используемой ОС, появление патчей, изготовленных производителями с целью устранения указанных уязвимостей, должно регламентироваться и производиться в плановом порядке.
- Установке патчей должно предшествовать тестирование информационной инфраструктуры на отсутствие негативных воздействий от вновь устанавливаемых патчей.
- В случае обнаружения негативного воздействия устанавливаемого патча на штатное функционирование информационной инфраструктуры, данный патч устанавливаться не должен.
- Установке новых версий ПО или внесению изменений и дополнений в действующее ПО должно предшествовать тестирование информационной инфраструктуры на отсутствие негативных воздействий указанного ПО.
- Установка протестированных патчей может быть произведена только на основании решения администратора безопасности.
- Установка новых версий ПО или внесение изменений и дополнений в действующее ПО может быть произведено только по согласованию с администратором безопасности.
- Применение организационно-технических и/или аппаратно-программных решений может быть произведено только по согласованию с администратором безопасности.

3. Контроль

Контроль за выполнением требований Настоящих Правил должен осуществлять администратор безопасности.

Приложение 4

Порядок работы с электронным журналом обращений пользователей информационной системы к ПДн

1. Общие положения

Правила и порядок протоколирования и анализа (аудита) значимых событий в ИСПДн, направлены на превентивную фиксацию и изучение действий субъектов и объектов в ИСПДн.

Все события, происходящие в ОС, ИСПДн, других критических приложений и СЗИ должны протоколироваться в специальные электронные журналы аудита.

Аудит событий, зафиксированных в указанных электронных журналах, должен анализироваться в плановом порядке на постоянной основе.

2. Настройки безопасности систем аудита

Электронные журналы аудита должны записываться и вестись в автоматизированном режиме.

Настройки журналов аудита должны однозначно интерпретировать все значимые события ИСПДн.

Электронные журналы аудита не должны быть доступны на чтение, уничтожение и модификацию пользователям ИСПДн.

Электронные журналы аудита не должны быть доступны на уничтожение и модификацию администраторам ИСПДн.

Электронные журналы аудита должны быть доступны на чтение и архивирование сотруднику, выполняющему функции администратора безопасности.

Размер каждого электронного журнала составляет 16 Мб. Затирание старых событий журнала происходит по необходимости по мере заполнения журнала.

3. Контроль

Контроль выполнения положений и требований порядка работы с электронным журналом обращений пользователей информационной системы к ПДн должен осуществлять администратор безопасности.

Приложение 5

Порядок предоставления информации органам государственной власти и местного самоуправления, физическим и юридическим лицам

1. Общие положения

Оператор должен предоставлять информацию, содержащую ПДн субъекта, третьим лицам только с письменного согласия субъекта ПДн за исключением случаев, предусмотренных частью 2 статьи 9 Федерального Закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

Информация, содержащая ПДн субъекта и предоставляемая третьим лицам, должна быть достоверной и не избыточной, по отношению к целям, заявленным этими лицами, при сборе ПДн.

При передаче обработки ПДн другому лицу на основании договора, оператор должен зафиксировать в нем обязанность указанного лица в обеспечении конфиденциальности ПДн и безопасности данных при их обработке.

2. Трансграничная передача данных

При трансграничной передаче ПДн оператор должен руководствоваться положениями статьи 12 ФЗ № 152 «О персональных данных».

Приложение 6

Порядок проведения служебного расследования нарушений режима информационной безопасности ИСПДн

1. Общие положения

Данный порядок устанавливает правила классификации нарушений информационной безопасности и процедуры служебного расследования (назначения, проведения и выработки выводов) для определения уровня защищенности ИСПДн оператора и мер по возможному предотвращению инцидентов информационной безопасности.

2. Классификация инцидентов информационной безопасности

Нарушения режима информационной безопасности и их последствия классифицируются по значимости на:

- Нарушения I категории.
- Нарушения II категории.
- Нарушения III категории.

Служебное расследование назначается по нарушениям I и II категорий.

3. Перечень инцидентов информационной безопасности

Инциденты I категории, к каковым относятся нарушения, повлекшие за собой разглашение (утечку) защищаемых ПДн и/или утрату содержащих их отчуждаемых носителей, уничтожение (искажение) ИСПДн, выведение из строя технических и программных средств, а именно:

- подбор административного пароля (успешный);
- несанкционированная реконфигурация параметров ИСПДн;
- утрата или кража резервной копии базы ПДн;
- необоснованная передача массивов ПДн;
- умышленное нарушение работоспособности ИСПДн;
- несанкционированный доступ к ПДн ИСПДн;
- несанкционированное внесение изменений в ИСПДн;
- умышленное заражение компьютеров и серверов ИСПДн вирусами;
- проведение работ с ИСПДн, повлекшее за собой необратимую потерю данных.

Инциденты II категории, к каковым относятся: нарушения, в результате которых возникают предпосылки к разглашению (утечке) защищаемых ПДн, утрате содержащих их отчуждаемых носителей, уничтожению (искажению) ИСПДн, выведению из строя технических и программных средств, а именно:

- ошибка при входе в ИСПДн (набор не назначенного пароля, более трех раз подряд, периодически);
- несанкционированное (неоднократное) оставление включенного ПК;
- перезагрузка компьютера, при сбоях в работе ПК, (неоднократная) в т.ч. аварийная (неоднократная) перезагрузка, путем нажатия кнопки RESET;
- утрата учтенного отчуждаемого съемного носителя;
- попытка входа под чужим именем, паролем, многократная неудачная;
- попытка входа под чужим именем пользователя, паролем, удачная;
- несанкционированная очистка журналов аудита;
- несанкционированное копирование ПДн на внешние носители;
- несанкционированная установка (удаление) ПО ИСПДн;
- несанкционированное изменение конфигурации ПО ИСПДн;

– попытка получения прав администратора на локальном ПК (увеличения собственных прав, получение прав на отладку программ) удачная и неудачная;

– попытка получения прав администратора в домене или на удаленной машине удачная и неудачная;

– неумышленное заражение локального или сетевого ПК компьютерными вирусами;

– несанкционированное использование сканирующего ПО;

– несанкционированное использование анализаторов протоколов (снифферов);

– несанкционированный просмотр, вывод на печать и т.п. ПДн.

Инциденты III категории, к каковым относятся нарушения, не несущие признаков нарушений I и II категорий, а именно:

– ошибка при входе в ИСПДн (набор неправильного пароля, сетевого имени более трех раз подряд, не периодическая);

– попытка неудачного доступа к ПДн ИСПДн (периодическая);

– перевод времени на ПК;

– выполнение собственных производственных обязанностей на компьютере в неразрешенное время;

– перезагрузка компьютера, при сбоях в работе ПК, (однократная) в т.ч. аварийная перезагрузка, путем нажатия кнопки RESET;

– нецелевое использование корпоративных ресурсов (печать, Internet, mail, и т.п.).

4. Назначение и проведение служебного расследования

Служебное расследование назначается по нарушениям I и II категорий.

Состав комиссии, а также сроки проведения служебного расследования назначаются распоряжением сотрудника, ответственного за обеспечение безопасности персональных данных, по каждому отдельному факту нарушения или по факту группы нарушений.

Служебное расследование может быть инициировано на основании устного заявления, докладной или служебной записки любого сотрудника оператора по выявленному отдельному факту нарушения, либо по факту группы нарушений.

5. Состав комиссии для проведения служебного расследования

В состав комиссии входят лица, назначенные Приказом «О создании комиссии для организации работы по защите персональных данных».

В случае необходимости Председатель комиссии может привлекать к работе:

– администраторов управления информатизации и телекоммуникаций;

– непосредственного начальника нарушителя;

– экспертов из других подразделений;

– привлеченных специалистов организаций-лицензиатов.

6. Члены комиссии имеют право:

Требовать документального подтверждения факта нарушений информационной безопасности ИСПДн оператора.

Устанавливать причины допущенных нарушений любым из способов, не противоречащим законодательству РФ;

Брать письменные объяснения по поводу выявленных нарушений у любого сотрудника оператора.

7. Ответственность.

Ответственность за выявление и классификацию инцидента информационной безопасности, требующего проведения процедуры служебного расследования несет администратор безопасности.

Ответственность за назначение процедуры служебного расследования несет руководитель организации.

Ответственность за проведение процедуры служебного расследования несет сотрудник, ответственный за обеспечение безопасности персональных данных в ИСПДн оператора.

Ответственность за содержание, обоснованность, актуализацию Настоящего Порядка, а также надлежащее выполнение его положений несет администратор безопасности.

8. Оформление результатов работы комиссии

Результаты работы Комиссии должны быть оформлены в виде аналитического экспертного заключения на имя руководителя, ответственного за обеспечение безопасности персональных данных, с предложениями по необходимым организационным выводам, а также по расширению или дополнению «Примерного перечня нарушений».

Результатом работы Комиссии должен стать АКТ, в котором изложены:

- Документальное подтверждение факта нарушений информационной безопасности ИСПДн оператора;
- установленные причины выявленных нарушений в ИСПДн оператора;
- сформированные предложения по устранению причин выявленных инцидентов информационной безопасности в ИСПДн оператора»;
- предложения по расширению (дополнению) «Перечня инцидентов информационной безопасности».

Приложение 7

Порядок приостановки предоставления доступа к ПДн в случае обнаружения нарушений порядка их обработки

1. Общие положения

Целью установления Настоящего Порядка является предотвращение утечки и несанкционированного доступа к ПДн при выявлении нарушений режима безопасности при обработке и/или чтении ПДн в ИСПДн.

Работа с ПДн должна приостанавливаться только при обнаружении нарушений I и/или II категорий.

2. Действие должностных лиц в случае обнаружения нарушений

Сотрудник, обнаруживший нарушения при работе с ПДн обязан сообщить об этом своему непосредственному руководителю.

Сотрудник, ответственный за обеспечение безопасности персональных данных в ИСПДн оператора, обязан:

- установить категорию выявленного нарушения;
- при установлении I или II категории нарушения инициировать проведение служебного расследования;
- оповестить все отделы и сотрудников, работающих с ПДн о прекращении доступа к ресурсам ИСПДн на время проведения служебного расследования.

Все отделы и сотрудники, работающие с ПДн обязаны:

- временно (на время проведения служебного расследования) приостановить свою деятельность по работе с ИСПДн;
- содействовать проведению служебного расследования.

Работа с ПДн может возобновляться только после устранения всех выявленных нарушений, их последствий;

Информация о возможности возобновления работы с ИСПДн должна доводиться до всех заинтересованных подразделений лицом, установившим запрет на работы в ИСПДн.

Приложение 8

Инструкция по организации резервирования и восстановления программного обеспечения, баз персональных данных информационных систем персональных данных в ПОО ЧУ «Юридический техникум» г. Кропоткин

1. Общие требования

1.1. Настоящая инструкция разработана в соответствии с требованиями подпункта «г» пункта 11 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781, с целью обеспечения возможности незамедлительного восстановления персональных данных (далее – ПДн), модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

1.2. Инструкция определяет правила и объемы резервирования, а также порядок восстановления работоспособности информационных систем персональных данных (далее – ИСПДн) ПОО ЧУ «Юридический техникум» г. Кропоткин (далее – оператор).

2. Резервируемое общесистемное и специальное программное обеспечение, программное обеспечение средств защиты информации и базы персональных данных

2.1. Необходимо осуществлять резервное копирование актуальной информации и данных, используемых для полного восстановления СУБД, содержащих персональные данные.

2.2. Резервное копирование осуществляется во внешнее хранилище (сервер резервного копирования, ЖМД, ГМД, CD-ROM, USB накопитель).

2.3. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль в соответствии с инструкцией по антивирусной защите.

3. Порядок резервирования и хранения резервных копий (ответственный за резервирование, периодичность)

3.1 Ежедневно, по окончанию работы с ПДн на ПЭВМ, должно осуществляться резервное копирование актуальных ПДн во внешнее хранилище, создавая тем самым резервный электронный архив актуальных ПДн.

3.2 Еженедельно, в пятницу, по окончании рабочего дня, должно осуществляться полное копирование данных, необходимых для восстановления работы СУБД, содержащих ПДн, во внешнее хранилище.

3.3 Электронные носители, на которые осуществляется резервное копирование актуальных ПДн и их копии должны быть поставлены на соответствующий учет.

3.4 Электронные носители, на которые осуществляется резервное копирование актуальных ПДн, должны храниться в специально оборудованном для хранения месте, обеспечивающем сохранность этих носителей.

3.5 Ответственность за организацию резервного копирования в ИСПДн в соответствии с требованиями настоящей Инструкции возлагается сотрудника, ответственного за обеспечение безопасности персональных данных в ИСПДн оператора.

3.6 Ответственность за проведение мероприятий резервного копирования в ИСПДн и соблюдение требований настоящей Инструкции возлагается на администратора безопасности и всех пользователей ИСПДн.

4. Порядок восстановления работоспособности ИСПДн

4.1 В случае потери работоспособности ИСПДн, должно быть обеспечено ее восстановление из резервной копии.

4.2 Восстановление из резервной копии осуществляется в соответствии с документацией, прилагающейся к системе резервного копирования ПО.

Лист ознакомления с «Положением по организации и проведению работ по обеспечению безопасности персональных данных» № 018 от «01» сентября 2016 г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	
«___» ______________ 20___ г.	