ФЕДЕРАЛЬНАЯ УПОЛНОМОЧЕННАЯ ОРГАНИЗАЦИЯ

АКЦИОНЕРНОЕ ОБЩЕСТВО
«УНИВЕРСАЛЬНАЯ ЭЛЕКТРОННАЯ КАРТА»
(АО «УЭК»)

УТВЕРЖДЕНО
Решением Правления АО «УЭК»
(Протокол № 139 от
22 марта 2017 г.)

П О Л И Т И К А

компании в отношении обработки персональных данных

Москва 2017

Содержание

Термины и определения

В настоящем документе используются следующие термины и их определения.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информацию или ресурсы информационной системы.

Доступность информации – свойство безопасности информации, при котором субъекты доступа, имеющие права доступа, могут беспрепятственно их реализовать.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация, обрабатываемая в информационной системе.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных, и обеспечивающих их обработку информационных технологий и технических средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информация ограниченного доступа – информация, доступ к которой ограничен федеральными законами.

Конфиденциальность информации – свойство безопасности информации, при котором доступ к ней осуществляют только субъекты доступа, имеющие на него право.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределённое программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему и (или) выходящей из информационной системы.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит своё отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых невозможно определить без использования дополнительной информации принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Общедоступная информация – это общеизвестные сведения и иная информация, доступ к которой не ограничен.

Оператор информационной системы – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы,

самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Техническое средство – аппаратное или программно-аппаратное устройство, осуществляющее формирование, обработку, передачу или прием информации в информационной системе.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, приём и обработку информативных сигналов.

Персональные данные (ПДн) – любая информация, относящаяся к определённому или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Политика «чистого стола» – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

Пользователь – лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в информационной системе или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Средства вычислительной техники (СВТ) – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – пользователь, процесс, выполняющие операции (действия) над объектами доступа и действия которых регламентируются правилами разграничения доступа.

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому или иностранному юридическому лицу.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных и (или) результате которых уничтожаются материальные носители персональных данных.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – свойство безопасности информации, при котором отсутствует любое ее изменение либо изменение субъектами доступа, имеющими на него право.

Обозначения и сокращения

АО «УЭК»	–	Акционерное общество «Универсальная электронная карта»
АРМ	–	Автоматизированное рабочее место
АВЗ	–	Антивирусная защита
ИБ	–	Информационная безопасность
ИС	–	Информационная система
ИСПДн	–	Информационная система персональных данных
КС	–	Корпоративная сеть Оператора
ЛВС	–	Локальная вычислительная сеть
НПА РФ	–	Нормативные правовые акты Российской Федерации
НСД	–	Несанкционированный доступ
ОРД	–	Организационно-распорядительная документация
ОС	–	Операционная система
ПДн	–	Персональные данные
ПО	–	Программное обеспечение
СЗИ	–	Средства защиты информации
СЗПДн	–	Система (подсистема) защиты персональных данных
СКЗИ	–	Средства криптографической защиты информации
СУБД	–	Система управления базами данных
ТС	–	Технические средства
УБИ	–	Угрозы безопасности информации
ФЗ-152	–	Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»
ФСБ России	–	Федеральная служба безопасности Российской Федерации
ФСТЭК России	–	Федеральная служба по техническому и экспортному контролю

Введение

Политика компании в отношении обработки персональных данных (далее — Политика) является официальным документом акционерного общества «Универсальная электронная карта» (далее — АО «УЭК», Оператор), в котором определена система взглядов на обеспечение информационной безопасности для информационных систем персональных данных (далее — ИСПДн) АО «УЭК».

Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее – информация), обрабатываемой в ИСПДн, изложенными в Концепции информационной безопасности АО «УЭК».

Политика разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановления Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и приказа ФСТЭК России № 21 от 18 февраля 2013 г. «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

В Политике определены требования к персоналу ИСПДн, степень ответственности персонала, структура и необходимый уровень защищённости ИСПДн, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности информации ИСПДн.

1. Общие положения

Целью настоящей Политики является обеспечение безопасности объектов защиты ИСПДн от всех видов угроз, внешних и внутренних, умышленных и не преднамеренных, минимизация ущерба от возможной реализации угроз безопасности информации (далее – УБИ).

Безопасность информации достигается путём исключения несанкционированного, в том числе случайного, доступа к информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение информации, а также иных несанкционированных действий.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБИ.

Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций, или уничтожений данных.

Компания обязана опубликовать или иным образом обеспечить неограниченный доступ к настоящей Политике обработки персональных данных в соответствии с ч. 2 ст. 18.1. ФЗ-152.

Настоящая Политика определяет порядок обработки персональных данных (далее — ПДн, персональных данных) и меры по обеспечению безопасности ПДн в АО «УЭК» с целью защиты прав и свобод человека и гражданина при обработке его ПДн, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

2. Область действия

Требования настоящей Политики распространяются на всех сотрудников АО «УЭК» (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

В Концепции информационной безопасности определены основные категории пользователей. На основании этих категории должна быть произведена типизация пользователей ИСПДн, определён их уровень доступа и возможности.

2.1. Пользователи ИСПДн

В ИСПДн можно выделить следующие группы пользователей, участвующих в обработке и хранении защищаемой Информации:

- Администратор ИСПДн;
- Администратор информационной безопасности (далее — Администратор ИБ);
- Пользователь ИСПДн;
- Технический специалист по обслуживанию периферийного оборудования;
- Программист-разработчик ИСПДн.

Данные о группах пользователях, уровне их доступа и информированности должны быть отражены в «Положении о разграничении прав доступа к обрабатываемой информации ограниченного доступа».

2.2. Должностные обязанности пользователей ИСПДн

Должностные обязанности пользователей ИСПДн описаны в следующих документах:

- Инструкция администратора ИСПДн;
- Инструкция Администратора ИБ;
- Инструкция пользователя ИСПДн;
- Инструкция Ответственного за обработку персональных данных.

3. Система защиты информации

Система защиты персональных данных (далее – СЗПДн) строится на основании:

- Отчёта о результатах обследования АО «УЭК в части выполнения требований законодательства Российской Федерации по вопросам обеспечения информационной безопасности в ИСПДн;
- Перечень ИСПДн в АО «УЭК»;
- Актов классификации;
- Положения о разграничении прав доступа к обрабатываемой информации ограниченного доступа;
- Руководящих документов ФСБ России и ФСТЭК России.

На основании этих документов определяется необходимый уровень значимости информации, обрабатываемой в ИСПДн. На основании анализа актуальных УБИ, описанных в Отчёте о результатах обследования ИСПДн, делается заключение о необходимости использования ТС и организационных мероприятий для обеспечения безопасности информации.

Для ИСПДн должен быть составлен перечень используемых ТС, а также программного обеспечения участвующего в обработке Информации, на всех элементах ИСПДн: АРМ пользователей; серверы приложений; СУБД; граница ЛВС; каналов передачи в сети общего пользования и (или) международного обмена, если по ним передается защищаемая информация.

В зависимости от класса защищённости ИСПДн и актуальных угроз, СЗПДн может включать следующие технические СЗИ:

- антивирусные средства для рабочих станций пользователей и серверов;
- средства межсетевого экранирования;
- СКЗИ при передаче защищаемой информации по каналам связи и т.д.

Так же в перечень должны быть включены функции защиты, обеспечиваемые штатными средствами обработки защищаемой информации ОС, прикладным ПО и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защиту машинных носителей информации;
- регистрацию событий безопасности;
- антивирусную защиту;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;
- целостность ИС и информации; доступность информации;
- защиту среды виртуализации; защиту ТС;
- защиту ИС, ее средств, систем связи и передачи данных.

4. Принципы и условия обработки персональных данных

4.1. Принципы и условия обработки ПДн

Обработка ПДн у Оператора осуществляется на основе следующих принципов:

- законности и справедливой основы;
- ограничения обработки ПДн достижением конкретных, заранее определенных и законных целей;
- недопущения обработки ПДн, несовместимой с целями сбора персональных данных;
- недопущения объединения баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой;
- обработки только тех ПДн, которые отвечают целям их обработки;
- соответствия содержания и объема обрабатываемых персональных данных заявленным целям обработки;
- недопущения обработки ПДн, избыточных по отношению к заявленным целям их обработки;
- обеспечения точности, достаточности и актуальности ПДн по отношению к целям обработки персональных данных;
- уничтожения либо обезличивания ПДн по достижении целей их обработки или в случае утраты необходимости в достижении этих целей, при невозможности устранения Оператором допущенных нарушений персональных данных, если иное не предусмотрено федеральным законом.

Оператор производит обработку ПДн при наличии хотя бы одного из следующих условий:

- обработка ПДн осуществляется с согласия субъекта ПДн;
- обработка ПДн необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;
- обработка ПДн необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;
- обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем;

- обработка ПДн необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн;
- обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно;
- осуществляется обработка ПДн, доступ неограниченного круга лиц к которым предоставлен субъектом ПДн либо по его просьбе (далее – общедоступные персональные данные);
- осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

4.2. Конфиденциальность ПДн

Оператор и иные лица, получившие доступ к ПДн, обязаны не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом.

4.3. Общедоступные источники ПДн

В целях информационного обеспечения у Оператора могут создаваться общедоступные источники персональных данных субъектов ПДн, в том числе справочники и адресные книги. В общедоступные источники персональных данных с письменного согласия субъекта ПДн могут включаться его фамилия, имя, отчество, дата и место рождения, должность, номера контактных телефонов, адрес электронной почты и иные персональные данные, сообщаемые субъектом ПДн.

Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта ПДн, уполномоченного органа по защите прав субъектов ПДн либо по решению суда или иных уполномоченных государственных органов.

4.4. Специальные категории ПДн и биометрические ПДн

Обработка Оператором ***специальных категорий ПДн***, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, допускается в случаях, если:

- субъект ПДн дал согласие в письменной форме;
- персональные данные сделаны общедоступными субъектом ПДн;
- обработка ПДн осуществляется в соответствии с законодательством государственной социальной помощи, трудовым законодательством, пенсионным законодательством Российской Федерации;
- обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта ПДн невозможно;

- обработка ПДн осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;
- обработка ПДн необходима для установления или осуществления прав субъекта ПДн или третьих лиц, а равно и в связи с осуществлением правосудия;
- обработка полученных в установленных законодательством Российской Федерации случаях персональных данных осуществляется органами прокуратуры в связи с осуществлением ими прокурорского надзора;
- обработка ПДн осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;
- обработка ПДн осуществляется в соответствии с законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации;
- обработка ПДн осуществляется в случаях, предусмотренных законодательством Российской Федерации, государственными органами, муниципальными органами или организациями в целях устройства детей, оставшихся без попечения родителей, на воспитание в семьи граждан;
- обработка ПДн осуществляется в соответствии с законодательством Российской Федерации о гражданстве Российской Федерации.

Обработка специальных категорий ПДн, осуществлявшаяся в случаях, изложенных выше должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась их обработка, если иное не установлено федеральным законом.

Обработка ПДн о судимости может осуществляться Оператором исключительно в случаях и в порядке, которые определяются в соответствии с федеральными законами.

Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность — ***биометрические персональные данные*** - могут обрабатываться Оператором только при наличии согласия субъекта ПДн в письменной форме.

4.5. Поручение обработки ПДн другому лицу

Оператор вправе поручить обработку ПДн другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора. Лицо, осуществляющее обработку ПДн по поручению Оператора, обязано соблюдать принципы и правила обработки ПДн, предусмотренные ФЗ-152 и настоящей Политикой.

4.6. Трансграничная передача ПДн

Оператор обязан убедиться в том, что иностранным государством, на территорию которого предполагается осуществлять передачу ПДн, обеспечивается адекватная защита прав субъектов персональных данных, до начала осуществления такой передачи.

Трансграничная передача ПДн на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов ПДн, может осуществляться в случаях:

- наличия согласия в письменной форме субъекта ПДн на трансграничную передачу;
- защиты жизни, здоровья, иных жизненно важных интересов субъекта ПДн или других лиц при невозможности получения согласия в письменной форме субъекта ПДн;
- исполнения договора, стороной которого является субъект ПДн.

5. Права субъекта ПДн

Субъект ПДн имеет право на получение у Оператора информации, касающейся обработки его ПДн, если такое право не ограничено в соответствии с федеральными законами. Субъект ПДн вправе требовать от Оператора уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Обработка ПДн в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с субъектом ПДн (потенциальным потребителем) с помощью средств связи, а также в целях политической агитации допускается только при условии предварительного согласия субъекта ПДн.

Оператор обязан немедленно прекратить по требованию субъекта ПДн обработку его персональных данных в вышеуказанных целях.

Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных федеральными законами, или при наличии согласия в письменной форме субъекта ПДн.

Если субъект ПДн считает, что Оператор осуществляет обработку его персональных данных с нарушением требований ФЗ-152 или иным образом нарушает его права и свободы, субъект ПДн вправе обжаловать действия или бездействие Оператора в Уполномоченный орган по защите прав субъектов ПДн или в судебном порядке.

Субъект ПДн имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда.

5.1. Согласие субъекта ПДн на обработку его персональных данных

Субъект ПДн принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных может быть дано субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом.

6. Положения политики

6.1. Политика физической безопасности

Все помещения Оператора должны отвечать требованиям НПА РФ в части оборудования устройствами сигнализации (например, пожарной, охранной и т.п.).

Помещения, которые должны быть оборудованы дополнительными устройствами регистрации, контроля и поддержания заданных характеристик (например, система автоматического пожаротушения, контроля влажности, принудительной вентиляции, кондиционирования воздуха, защиты от статического электричества и т.п.), в соответствии с НПА РФ или правилами эксплуатации оборудования, размещенного в таких помещениях, и требуемых для соблюдения гарантийных обязательств производителя, должны быть полностью укомплектованы подобными устройствами.

В «Политику физической безопасности» входят такие процедуры и процессы, как:

1) Организация охраны
2) Контроль доступа
3) Контроль нахождения посторонних лиц в помещениях Оператора
4) Эксплуатация электронных устройств
5) Ограничения при эксплуатации
6) Профилактическое обслуживание и иные правила эксплуатации
7) Прекращение эксплуатации

6.2. Политика обеспечения управления доступом

Сотрудникам АО «УЭК» запрещено осуществление противоправных действий:

- по получению несанкционированного доступа к любой АС;
- по нанесению ущерба и нарушению работы АС;
- по перехвату паролей или иному способу получения паролей, ключевой информации или иных механизмов доступа, которые могут быть использованы для НСД.

ПО, предполагающее использование механизмов разделения доступа или подразумевающее индивидуальную ответственность сотрудника за осуществляемые действия, должно использовать механизм контроля доступа, с идентификацией и авторизацией пользователя с помощью, как минимум пароля, отвечающего требованиям политики парольной защиты.

Доступ к информации ограниченного доступа должен соответствовать требованиям НПА РФ и ОРД АО «УЭК».

Меры безопасности, используемые на АРМ и в КС, должны быть просты для использования, управления и аудита.

Настройка доступа ко всем информационным ресурсам Оператора должна быть по умолчанию направлена на предотвращение к ним любого НСД.

Если система контроля доступа АРМ, КС или АС вышла из строя, то доступ пользователей должен быть запрещен до решения проблемы.

До предоставления прав доступа к информационным ресурсам АО «УЭК», пользователь должен быть ознакомлен под роспись с ОРД Оператора, регламентирующими работу с конкретными информационными ресурсами. В случаях, когда это определено необходимостью или требованиями НПА РФ, или ОРД Оператор должен быть проведен дополнительный инструктаж или обучение. Факт проведения инструктажа или обучения должен быть закреплен в соответствии с требованиями документов, обуславливающих их проведение.

В случаях, когда это определено НПА РФ и ОРД Оператора, сотрудник помимо ознакомления, должен письменно подтвердить свое обязательство выполнять требования документов.

В «Политику обеспечения управления доступом» входят такие процедуры и процессы, как:

1) Общие правила доступа к КС Оператора
2) Создание Идентификатора учетной записи
3) Создание учетных записей специальных типов
4) Требования по настройке системы управления доступом
5) Требования безопасности по использованию системы управления доступа

6.3. Политика использования программного обеспечения

ПО, используемое для осуществления деятельности структурных подразделений Оператора, должно соответствовать условиям его лицензирования (независимо от того, является ли оно коммерческим или свободно распространяемым) и использоваться строго в соответствии с лицензионным соглашением. Любое структурное подразделение Оператора должно исключить случаи хранения и использования ПО, не являющегося лицензионным.

В случае если в НПА РФ предъявляются особые требования к ПО (например, требование по сертификации такого ПО уполномоченными организациям и т.п.), структурное подразделение Оператора обязано обеспечить выполнение подобных требований.

На каждое АРМ должен быть установлен комплект ПО, необходимый и достаточный для выполнения на нем поставленных задач.

Оператор предоставляет сотрудникам достаточное количество лицензий на использование ПО, необходимого для выполнения должностных обязанностей.

На технические средства, подключаемые к КС и подразумевающие возможность установки прикладного ПО, должно быть установлено базовое ПО, предусмотренное «Реестром программного обеспечения» и предназначенное к установке на ТС, подключаемых к КС.

Обновление версий ПО, использующего ресурсы КС, должно осуществляться только администраторами ИСПДн или уполномоченным лицом. Допустимо использование функции автоматического обновления ПО, использующего ресурсы КС.

6.4. Политика антивирусной защиты (АВЗ)

Антивирусное ПО должно быть установлено и функционировать в штатном режиме на всех компьютерах, выполняющих функции серверов КС, на всех АРМ отдельно стоящих и подключенных к КС и на всех портативных компьютерах.

Не допускается изменение настроек системы АВЗ, в части оповещения о нахождении компьютерных вирусов или вредоносных программ, в результате действия которых уменьшается эффективность работы ИС.

Обновления баз системы АВЗ должно производиться регулярно. Построение системы АВЗ должно предусматривать возможность обновления ее антивирусных баз и компонентов производителем по мере их создания. В случае невозможности такого построения системы (например, отдельно стоящие АРМ не подключенные к каким-либо сетям), обновление системы АВЗ должно производиться с регулярностью, обеспечивающей ее эффективное функционирование.

Запрещается отключение системы АВЗ, за исключением случаев проведения тестирования программного обеспечения и иных тестов, проводимых уполномоченными сотрудниками Оператора.

В «Политику антивирусной защиты» входят такие процедуры и процессы, как:

1) Предотвращение выполнения вредоносного кода
2) Обнаружение вредоносного кода

6.5. Политика «чистого стола» и «чистого экрана»

С целью минимизации риска неавторизованного доступа или повреждения документов на бумажных носителях, носителей данных и средств обработки информации, рекомендуется внедрить в АО «УЭК» политику «чистого стола» и «чистого экрана».

Оператору следует применять политику «чистого стола» в отношении документов на бумажных носителях и сменных носителей данных, а также политику «чистого экрана» в отношении средств обработки информации с тем, чтобы уменьшить риски неавторизованного доступа, потери и повреждения информации как во время рабочего дня, так и при внеурочной работе. При применении этих политик следует учитывать соответствующие риски, а также корпоративную культуру организации.

Носители информации, оставленные на столах, также могут быть повреждены или разрушены при бедствии, например, при пожаре, наводнении или взрыве.

Следует применять следующие мероприятия по управлению информационной безопасностью:

- чтобы исключить компрометацию информации, целесообразно бумажные и электронные носители информации, когда они не используются, хранить в надлежащих запирающихся шкафах и/или в других защищенных предметах мебели, а так же в архивах Оператора, особенно в нерабочее время;
- носители с важной или критичной служебной информацией, когда они не требуются, следует убирать и запирать (например, в несгораемом сейфе или металлическом шкафу), особенно когда помещение пустует;

- персональные компьютеры и принтеры должны быть выключены по окончании работы;
- следует применять кодовые замки, пароли или другие мероприятия в отношении устройств, находящихся без присмотра;
- в нерабочее время фотокопировальные устройства следует запирать на ключ (или защищать от неавторизованного использования другим способом);
- напечатанные документы с важной или конфиденциальной информацией необходимо изымать из принтеров немедленно.

6.6. Политика использования электронных носителей

Сотрудники, которым необходимо использование электронных носителей информации для выполнения должностных обязанностей, должны быть обеспечены Оператором такими носителями. Использование личных электронных носителей информации сотрудников для выполнения должностных обязанностей разрешено, при условии выполнения требований политик безопасности. Необходимость использования сотрудником личных электронных носителей информации должна быть сведена к минимуму.

Служебные электронные носители информации должны подлежать учету и выдаваться сотрудникам под роспись. Сотрудник несет персональную ответственность за их сохранность. Сотрудникам запрещено создавать предпосылки для осуществления утраты, кражи и иных противоправных действий со служебными электронными носителями информации.

Использование электронных носителей информации для хранения информации ограниченного доступа должно соответствовать требованиям НПА РФ и внутренних документов Оператора.

Использование служебных электронных носителей информации в личных целях запрещено.

Подключение служебных электронных носителей информации к ТС, заведомо содержащим вирусы или вредоносные программы, запрещено. В этом случае электронные носители передаются Администратору ИБ.

Эксплуатация электронных носителей информации должна осуществляться в соответствии с требованиями по их эксплуатации, и направлена на предупреждение их неисправности.

6.7. Политика использования средств криптографической защиты информации (СКЗИ)

Деятельность со СКЗИ должна исключать нарушение законодательства Российской Федерации в области лицензирования. В случае, если предполагаемая деятельность со СКЗИ подразумевает необходимость получения лицензии, то Оператор обязан получить такую лицензию или привлекать для подобной деятельности сторонние организации, имеющие соответствующие лицензии.

При использовании СКЗИ для защиты информации ограниченного доступа данные криптографические средства должны соответствовать требованиям НПА РФ.

Установка, настройка и техническое сопровождение СКЗИ должно осуществляться квалифицированными специалистами и не нарушать требования НПА РФ.

Использование, в том числе хранение, СКЗИ должно отвечать требованиям законодательства Российской Федерации.

Перед использованием СКЗИ сотрудники обязаны пройти обучение по порядку их использования.

Пользователям запрещено использование СКЗИ других пользователей, в том числе с целью выдать себя за другого пользователя.

В «Политику СКЗИ» входят такие процедуры и процессы, как:

1) Предотвращение компрометации ключей
2) Ведение журнала учета СКЗИ

6.8. Политика резервного копирования

Резервное копирование информации, размещенной на АРМ сотрудников и компьютерах, выполняющих функции сервера КС, осуществляется уполномоченным лицом Оператора.

В «Политику резервного копирования» входят такие процедуры и процессы, как:

1) Порядок резервного копирования рабочей информации
2) Регламентирование резервного копирования и восстановление информации
3) Порядок хранения резервных копий

6.9. Политика парольной защиты

Доступ к ПО, используемому пользователями и администраторами в рамках должностных обязанностей и подразумевающему наличие идентификации и аутентификации пользователя и разграничение полномочий, без использования пароля запрещено.

Пароли доступа к различному прикладному ПО, используемому пользователями и администраторами в рамках должностных обязанностей должны отличаться от паролей доступа к АРМ или элементам сетевой инфраструктуры и не должны совпадать для различного ПО.

Администраторам запрещено отклоняться от настоящей политики во имя удобства пользования.

В «Политику парольной защиты» входят такие процедуры и процессы, как:

1) Порядок создания пароля
2) Регулярность смены пароля
3) Восстановление пароля
4) Хранение пароля и передача его третьим лицам

6.10. Политика обеспечения сетевой безопасности

Конфигурация и настройка всех устройств, подключенных к КС должны соответствовать требованиям НПА РФ и ОРД Оператора.

Размещение в КС информации ограниченного доступа должно соответствовать требованиям НПА РФ и ОРД Оператора.

Используемые внешние интерфейсы и протоколы КС должны быть максимально ограничены необходимыми для обеспечения выполнения Оператором своих задач и функций.

ТС, обеспечивающие работу КС, должны размещаться с соблюдением требований по контролю физического доступа к ним и организации их сохранности. Доступ к серверам лиц, не уполномоченных для работы с данным оборудованием, должен быть исключен или осуществляться в сопровождении уполномоченных сотрудников Оператора.

Использование для подключения и управления техническими средствами протокола *Telnet* запрещено. Для управления техническими устройствами в сети по возможности должен быть использован протокол *SSH*.

В «Политику обеспечения сетевой безопасности» входят такие процедуры и процессы, как:

1) Построение КС Оператора
2) Обеспечение безопасности маршрутизаторов
3) Ограничения по использованию КС Оператора

6.11. Политика использования сети Интернет и электронной почты

Вся информация, полученная из сети Интернет, должна считаться недостоверной, не будучи подтвержденной из других источников. Перед использованием свободно распространяемой информации из сети Интернет для принятия решений в рамках деятельности АО «УЭК», такая информация должна быть перепроверена в других источниках.

Оператор не несет ответственности за информацию, содержащуюся в сети Интернет. В случае открытия пользователем ресурсов, содержание которых может считаться незаконным или оскорбительным, например, материалы сексуального характера, расистские, дискредитирующие, оскорбительные, непристойные, уничижительные, дискриминационные, угрожающие, пользователь обязан прекратить работу с данным ресурсом.

В «Политику обеспечения сетевой безопасности» входят такие процедуры и процессы, как:

1) Обеспечение безопасности использования сети Интернет
2) Ограничение предоставления доступа к сети Интернет
3) Ограничения использования сети Интернет

Электронная почта должна быть использованы сотрудниками Оператора только для выполнения должностных обязанностей, выполнения договорных обязательств Оператора и выполнения требований НПА РФ.

Запрещено использовать электронную почту для отправления писем следующего содержания:

- писем, содержание которых может считаться незаконным или оскорбительным, например, материалы сексуального характера, расистские, дискредитирующие, непристойные, уничижительные, угрожающие, или иные подобные сообщения;
- любых подрывных, неэтичных, незаконных или недопустимых материалов, включая оскорбительные комментарии по поводу расы, пола, цвета, инвалидности, возраста, сексуальной ориентации, порнографии, терроризма, религиозных убеждений и верований, политических убеждений или о национальном происхождении, гиперссылок или других ссылок на неприличные или очевидно оскорбительные веб-сайты и подобные материалы;
- писем, написанных таким образом, который может быть интерпретирован как официальная позиция или высказывание Оператора, если это не разрешено директором в соответствии с нормативно-методическими документами Оператора.

Запрещено использовать электронную почту в следующих целях:

- отправки сообщения с чужого почтового ящика или от чужого имени;
- отправки сообщений в личных или благотворительных целях, не связанных с деятельностью Оператора;
- отправки и пересылки писем, пересылаемых по цепочке («письма счастья»);
- массовой рассылки писем, кроме случаев, когда необходимо оповещение большого числа сотрудников Оператора или в случаях, когда это обусловлено выполнением задач АО «УЭК»;
- в любых других незаконных, неэтичных и неразрешенных целях.

Сотрудники Оператора, получившие электронную почту от другого сотрудника Оператора, с сообщениями, содержащими запрещенное содержание обязаны уведомить о таком факте директора и Администратора ИБ.

В «Политику использования электронной почты» входят такие процедуры и процессы, как:

1) Безопасность при использовании системы электронной почты
2) Безопасность при использовании архивных файлов
3) Безопасность при получении спама

6.12. Политика повышения осведомленности в области ИБ и кадровая политика

Проведение мероприятий, направленных на постоянное повышение осведомленности сотрудников Оператора в области ИБ, должна являться одной из задач, решаемых АО «УЭК».

Необходимо проведение периодического практического тестирования готовности сотрудников к выполнению своих должностных обязанностей по защите информации.

Конкретные требования по обеспечению ИБ должны быть внесены в должностные регламенты всех сотрудников Оператора, в зависимости от их должностных обязанностей.

Подбор, и порядок вступления в договорные и трудовые отношения и их расторжения, а также ежедневное выполнение сотрудником его должностных обязанностей, должны соответствовать требованиям НПА РФ и ОРД Оператора.

Порядок допуска сотрудника к работе с информацией ограниченного доступа, порядок работы с такой информацией и порядок прекращения допуска к такой информации, должен соответствовать НПА РФ и ОРД Оператора.

В «Политику повышения осведомленности в области ИБ и кадровую политику» входят такие процедуры и процессы, как:

1) Требования до приема на работу
2) Требования при выполнении должностных обязанностей
3) Требования при прекращении выполнения должностных обязанностей

7. Заключительные положения

В соответствии со ст. 17 Федерального закона Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» лица, виновные в нарушении требований данного Федерального закона, несут дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Настоящая Политика является внутренним документом Оператора и подлежит пересмотру, но не чаще одного раза в три года, а также изменению и дополнению в случае внесения изменений в действующее законодательство в области обработки и защиты персональных данных.

Пересмотр может быть вызван следующими причинами:

- Истечение времени действия политики.
- Изменения существующего технологического процесса.
- Появление нового технологического процесса.
- Изменение структуры или состава КС Оператора.
- Изменение информационных потоков.
- Обнаружение новых уязвимостей.
- Нарушение политик информационной безопасности.

Вследствие этого могут изменяться или создаваться новые политики, стандарты и руководства.

Контроль за соблюдением Политики осуществляет Президент АО «УЭК».

Настоящая Политика обязательна для соблюдения и подлежит доведению до всех работников, а также опубликованию на официальном сайте Оператора в течение 10-ти дней со дня утверждения.

Всего прошито, пронумеровано и скреплено печатью

(двадцать пять) лист 08

Президент АО «УЭК»

И.Н. Мамонтов

М.П.