ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
"ПРО-ЭКСПЕРТ"

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат 021A436A0060B2F0B1499C5EA3A256CC6F
Владелец Кузнецов Антон Варисович
Действителен с 09.01.2025 по 09.04.2026

УТВЕРЖДАЮ:
Директор ООО "ПРО-Эксперт"

_____ А.В. Кузнецов

ПОЛИТИКА БЕЗОПАСНОСТИ ООО "ПРО-ЭКСПЕРТ"

1. Общие положения

1.1. Настоящая Политика безопасности Общества с ограниченной ответственностью "ПРО-Эксперт" (далее – Политика) разработана в целях обеспечения защиты информационных ресурсов Общества с ограниченной ответственностью "ПРО-Эксперт" (далее – образовательная организация), а также защиты прав и свобод человека и гражданина при обработке его персональных данных, и действует в отношении всех данных, которые обрабатывает образовательная организация.

1.2. Настоящая Политика направлена на защиту информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий образовательной организации, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации, и обеспечение нормального функционирования технологических процессов.

1.3. Настоящая Политика разработана в соответствии с требованиями нормативных правовых актов:

- Конституция Российской Федерации;
- "Федеральный закон от 27.07.2006 №149-ФЗ "Об информации, информационных технологиях и о защите информации";
- Федеральный закон от 27.07.2006 №152-ФЗ "О персональных данных";
- Федеральный закон от 06.04.2011 №63-ФЗ "Об электронной подписи";
- Закон Российской Федерации от 07.12.1992 №2300-1 "О защите прав потребителей";

- Федеральный закон от 27.06.2011 №161-ФЗ "О национальной платежной системе";
- Федеральный закон от 30.12.2020 №491-ФЗ "О приобретении отдельных видов товаров, работ, услуг с использованием электронного сертификата";
- Федеральный закон от 22.10.2004 №125-ФЗ "Об архивном деле в Российской Федерации";
- Указ Президента Российской Федерации от 01.05.2022 №250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации";
- Постановление Правительства Российской Федерации от 01.11.2012 №1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
- иные нормативные правовые акты Российской Федерации.

2. Термины и определения

Автоматизированная система – это комплекс взаимосвязанных технических и программных средств, предназначенных для автоматизации задач управления или производственных процессов, включающий в себя аппаратное обеспечение, программное обеспечение и человеческий фактор, которые совместно обеспечивают сбор, обработку, хранение и передачу информации, необходимую для принятия решений и контроля над объектом управления.

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

Администратор информационной безопасности – специалист организации, осуществляющий контроль за обеспечением защиты информации, а также осуществляющий организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления несанкционированного доступа к защищаемой информации.

Аудит информационной безопасности – процесс проверки выполнения установленных требований по обеспечению информационной безопасности.

Аутентификация пользователя – проверка принадлежности субъекту доступа предъявленного им идентификатор (подтверждение подлинности).

Безопасность информации (данных) – состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность.

Блокирование информации – временное прекращение сбора, систематизации, накопления, использования, распространения информации, в том числе ее передачи.

Владелец информационного ресурса – лицо, самостоятельно и по своему усмотрению определяющее порядок использования сайта в сети "Интернет", в том числе порядок размещения информации на таком сайте.

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

Доступ к информации (данным) – возможность получения и использования информации (данных).

Защищаемая информация (защищаемые данные) – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями нормативных правовых актов и требованиями, установленными собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Информационная безопасность – состояние защищенности интересов организации в условиях угроз в информационной среде, при этом защищенность достигается обеспечением конфиденциальности, целостности, доступности информации.

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

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

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

Источник угрозы безопасности – субъект доступа, материальный объект или физическое явление, являющееся причиной возникновения угрозы безопасности информации.

Квалифицированный сертификат ключа проверки электронной подписи – сертификат ключа проверки электронной подписи, соответствующий требованиям Федерального закона от 06.04.2011 №63-ФЗ "Об электронной подписи", созданный аккредитованным удостоверяющим центром либо уполномоченным федеральным органом, и являющийся официальным документом.

Конфиденциальность информации (данных) – обязательное для выполнения лицом, получившим доступ к определенной информации, требования не передавать такую информацию третьим лицам без согласия ее обладателя.

Меры обеспечения безопасности – совокупность действий, направленных на разработку и (или) практическое применение способов и средств обеспечения информационной безопасности.

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

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

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

Объект доступа – единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

Объект защиты информации – информация либо носитель информации, или информационный процесс, которую (который) необходимо защищать в соответствии с целью защиты информации.

Оператор платежной системы – организация, определяющая правила платежной системы в соответствии с законодательством Российской Федерации.

Оператор по переводу денежных средств – организация, которая в соответствии с законодательством Российской Федерации вправе осуществлять перевод денежных средств.

Пароль – набор знаков (букв, цифр и других символов), предназначенный для подтверждения личности или полномочий. В компьютерных системах служит для получения доступа к данным и сервисам, является средством защиты от несанкционированного доступа.

Перевод денежных средств – действия оператора по переводу денежных средств в рамках применяемых форм безналичных расчетов по предоставлению получателю средств денежных средств плательщика.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Платежная (банковская) карта – пластиковая карта, привязанная к одному или нескольким расчетным (лицевым) счетам в банке. Используется для оплаты товаров (работ, услуг), в том числе через интернет, а также для снятия наличных средств.

Платежная система – совокупность организаций, взаимодействующих по правилам платежной системы в целях осуществления перевода денежных средств.

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

Предоставление информации (данных) – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

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

Программное воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Распространение информации (данных) – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Сайт в сети "Интернет" – совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети "Интернет" по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети "Интернет".

Сертификат ключа проверки электронной подписи - электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Система быстрых платежей (СБП) – сервис быстрых платежей платежной системы Банка России, способ оплаты за товары (работы, услуги), при котором оплата заказа производится в приложении участника СБП, подключенного к СБП. Оператором и расчетным центром СБП является Банк России.

Система защиты информации (данных) – совокупность организационных и технических мероприятий для защиты информации от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий с ней.

Система электронных платежей – комплекс специализированных программных средств, обеспечивающий транзакции (перевод) денежных средств от получателя услуг к поставщику услуг, где поставщик услуг имеет собственный расчетный счет (самые распространенные типы платежных систем: Visa и MasterCard).

Страница сайта в сети "Интернет" – часть сайта в сети "Интернет", доступ к которой осуществляется по указателю, состоящему из доменного имени и символов, определенных владельцем сайта в сети "Интернет".

Субъект доступа – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Третья сторона – лица или организация, которые признаны независимыми от участвующих сторон, по отношению к рассматриваемой проблеме.

Угрозы безопасности информации (данных) – совокупность условий и факторов, создающих опасность несанкционированного, в том числе

случайного, доступа к информации, результатом которого может стать ее уничтожение, изменение, блокирование, копирование, распространение, а также иных несанкционированных действий при ее обработке в информационных системах.

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

Целостность информации (данных) – способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях ее случайного и (или) преднамеренного искажения (разрушения).

Электронная подпись (ЭЦП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети.

Электронный сертификат – размещенная в Государственной информационной системе электронных сертификатов запись в электронной форме, содержащая сведения о праве гражданина Российской Федерации на самостоятельное приобретение отдельных видов товаров, работ, услуг за счет средств соответствующего бюджета бюджетной системы Российской Федерации и используемая для подтверждения оплаты таких товаров, работ, услуг в объеме, установленном законодательством Российской Федерации.

3. Информационная безопасность

3.1. Вся существенная информация в любой форме, приобретенная или полученная образовательной организацией и используемая для поддержки ее законной деятельности, принадлежит образовательной организации.

3.2. Для защиты ресурсов корпоративной системы и связанных с нею существенных данных от случайного или несанкционированного изменения, раскрытия или уничтожения, а также для обеспечения конфиденциальности, целостности и доступности информации и средств ее обработки, образовательная организация применяет меры по организационной безопасности и физической защите, технические меры безопасности.

3.3. Получение пользователями доступа к информационным ресурсам основывается на аутентификации этих пользователей и разграничении доступа.

3.4. Управление доступом к сетевым информационным ресурсам и услугам производится, в том числе, путем разделения информационной телекоммуникационной системы образовательной организации на отдельные логические и физические сетевые сегменты.

3.5. В целях выявления нецелевого использования средств обработки информации пользователями, несанкционированных действий третьих лиц, оперативного реагирования на инциденты информационной безопасности осуществляется мониторинг информационной безопасности.

3.6. Мониторинг информационной безопасности реализуется с использованием специальных средств обеспечения информационной безопасности, в том числе средств контроля доступа, регистрации событий и синхронизации времени.

4. Безопасность при использовании электронных платежных систем

4.1. Оплата предоставляемых образовательной организацией услуг осуществляется посредством сервиса Юkassa (далее – сервис оплаты).

4.2. Сервис оплаты позволяет осуществлять расчеты разными способами:

- с платежных (банковских) карт (Visa, Mastercard, Maestro, МИР);
- через интернет-банк (СБП);
- по электронному сертификату, привязанному к карте "МИР"[1].

4.3. При оплате пользователем услуг образовательной организации сервис оплаты обеспечивает безопасность расчетов. При совершении платежа, необходимая сумма денежных средств блокируется до подтверждения оплаты образовательной организацией. При отмене по какой-либо причине сделки, денежные средства возвращаются пользователю.

4.4. Прием платежей осуществляется через защищенное безопасное соединение, используя протокол HTTPS, который шифрует данные платежей. Протокол HTTPS соответствует стандарту НСПК, Visa и Mastercard (PCI DSS).

4.5. Соответствие сервиса оплаты Международному стандарту, регулирующему безопасность данных держателей платежных карт (PCI DSS), гарантирует, что:

- данные пользователей надежно шифруются при передаче;
- сайт образовательной организации защищен от вирусов и атак;

---

[1] Право на приобретение образовательных услуг с использованием электронного сертификата имеют отдельные категории граждан РФ в соответствии с Федеральным законом от 30.12.2020 №491-ФЗ "О приобретении отдельных видов товаров, работ, услуг с использованием электронного сертификата "

- у образовательной организации отсутствует доступ к информации о карте пользователя.

4.6. После успешного прохождения оплаты на электронную почту плательщика направляется электронная квитанция, подтверждающая совершение платежа и содержащая его уникальных идентификатор.

4.7. При оплате услуг банковской картой возврат денежных средств производится на ту же карту, с которой был произведен платеж.

5. Заключительные положения

5.1. Все вопросы, неурегулированные настоящей Политикой, решаются в соответствии с действующим законодательством Российской Федерации.

5.2. Настоящая Политика является внутренник документом образовательной организации, общедоступной и подлежит размещению на официальном сайте образовательной организации.

5.3. Настоящая Политика подлежит изменению, дополнению в случае изменения законодательства Российской Федерации.