

Пояснительная записка

по реализации инвестиционного проекта "Приобретение программного обеспечения для осуществления энергосбытовой деятельности"
(O_3.08_SOFT)

1. Цели реализации инвестиционного проекта.

Повышение уровня автоматизации процессов, связанных с энергосбытовой деятельностью, повышение уровня информационной безопасности, препятствование действиям злоумышленников, получение возможности обнаруживать признаки кибератак и оказывать противодействие злоумышленникам, соблюдение требований законодательства в области обеспечения информационной безопасности объектов критической информационной инфраструктуры и систем, обрабатывающих персональные данные.

2. Задачи реализации инвестиционного проекта.

Повышение надёжности осуществления энергосбытовой деятельности, повышение качества обслуживания потребителей (покупателей), автоматизация процессов, связанных с энергосбытовой деятельностью, повышение уровня информационной безопасности.

3. Описание результатов реализации инвестиционного проекта.

Внедрение биллинговой системы на базе программного комплекса "1С: Предприятие", приобретение антивирусного программного обеспечения, приобретение программного обеспечения "Платформа 1С x64 Prof", приобретение программного комплекса защиты персональных данных, приобретение программного комплекса выявления уязвимостей в информационных системах, приобретение программного комплекса контроля бесперебойной работы информационных систем.

4. Обоснование необходимости реализации инвестиционного проекта.

Необходимость реализации инвестиционного проекта обусловлена достижением целей повышения автоматизации процессов энергосбытовой деятельности при расчетах с потребителями электрической энергии (в том числе населением и приравненными к нему категориями потребителей), выполнения требований федерального законодательства в отношении

безопасности информационных систем, используемых в бизнес-процессах гарантирующего поставщика.

5. Период реализации инвестиционного проекта.

Планируемый период реализации инвестиционного проекта в рамках периода реализации инвестиционной программы (по годам): 2025, 2026, 2027, 2028, 2029 год(ы)

Год начала: 2025

Год окончания: 2029

6. Перечень мероприятий, предусмотренных инвестиционным проектом, с указанием количественных и стоимостных характеристик на весь период реализации инвестиционной программы (по годам).

Период реализации / Наименование мероприятия (объект ОС, НМА)	Единица измерения	Количество (если применимо)	Прогнозная стоимость, тыс. руб. без НДС
Перечень мероприятий 2025 года:			
Приобретение программного обеспечения "Платформа 1С х64 КОРП"	компл.	1	3 301,1
Приобретение программного комплекса защиты персональных данных (Федеральный закон от 27.07.2006 №152-ФЗ)	компл.	1	357,5
Приобретение программного комплекса выявления уязвимостей в информационных системах (Приказ ФСТЭК России от 18.02.2013 г. №21)	компл.	1	154,3
Приобретение программного комплекса контроля бесперебойной работы информационных систем (Приказ ФСТЭК России от 25.12.2017 г. №239)	компл.	250	4 950,7
Разработка биллинговой системы на базе программного комплекса "1С: Предприятие"	компл.	1	54 736,1

Период реализации / Наименование мероприятия (объект ОС, НМА)	Единица измерения	Количество (если применимо)	Прогнозная стоимость, тыс. руб. без НДС
Приобретение антивирусного программного обеспечения	компл.	1	518,6
Перечень мероприятий 2026 года:			
Приобретение программного комплекса защиты персональных данных (Федеральный закон от 27.07.2006 №152-ФЗ)	компл.	1	371,9
Приобретение программного комплекса выявления уязвимостей в информационных системах (Приказ ФСТЭК России от 18.02.2013 г. №21)	компл.	1	160,5
Приобретение программного комплекса контроля бесперебойной работы информационных систем (Приказ ФСТЭК России от 25.12.2017 г. №239)	компл.	250	5 150,2
Приобретение антивирусного программного обеспечения	компл.	1	539,5
Перечень мероприятий 2027 года:			
Приобретение программного комплекса защиты персональных данных (Федеральный закон от 27.07.2006 №152-ФЗ)	компл.	1	386,6
Приобретение программного комплекса выявления уязвимостей в информационных системах (Приказ ФСТЭК России от 18.02.2013 г. №21)	компл.	1	166,8
Приобретение программного комплекса контроля бесперебойной работы информационных систем (Приказ ФСТЭК России от 25.12.2017 г. №239)	компл.	250	5 354,5
Приобретение антивирусного программного обеспечения	компл.	1	560,9

Период реализации / Наименование мероприятия (объект ОС, НМА)	Единица измерения	Количество (если применимо)	Прогнозная стоимость, тыс. руб. без НДС
Перечень мероприятий 2028 года:			
Приобретение программного комплекса защиты персональных данных (Федеральный закон от 27.07.2006 №152-ФЗ)	компл.	1	402,1
Приобретение программного комплекса выявления уязвимостей в информационных системах (Приказ ФСТЭК России от 18.02.2013 г. №21)	компл.	1	173,5
Приобретение антивирусного программного обеспечения	компл.	1	583,3
Перечень мероприятий 2029 года:			
Приобретение программного комплекса защиты персональных данных (Федеральный закон от 27.07.2006 №152-ФЗ)	компл.	1	418,2
Приобретение программного комплекса выявления уязвимостей в информационных системах (Приказ ФСТЭК России от 18.02.2013 г. №21)	компл.	1	180,5
Приобретение антивирусного программного обеспечения	компл.	1	606,7

Расчет стоимости мероприятий, входящих в состав инвестиционного проекта, на период реализации проекта инвестиционной программы представлен в формате электронного документа (Excel) в составе обосновывающих материалов.

Обосновывающие документы в отношении ценовых параметров, используемых при расчете стоимости мероприятий, входящих в состав инвестиционного проекта, на период реализации проекта инвестиционной программы, представлены в формате электронных документов (PDF) в составе обосновывающих материалов.

7. Совокупная прогнозная стоимость реализации инвестиционного проекта на весь период реализации инвестиционной программы (по годам).

Период реализации	Прогнозная стоимость, тыс. руб. без НДС	Прогнозная стоимость, тыс. руб. с НДС
2025	64 018,1	64 018,1
2026	6 222,1	6 222,1
2027	6 468,9	6 468,9
2028	1 158,8	1 158,8
2029	1 205,3	1 205,3
ВСЕГО	79 073,2	79 073,2

8. Дополнительная информация к описанию мероприятий инвестиционного проекта.

8.1 Приобретение программного комплекса контроля бесперебойной работы информационных систем (Приказ ФСТЭК России от 25.12.2017 г. №239).

8.1.1 Цели реализации.

- выявление, анализ, хранение и защита информации об инцидентах;
- оперативное реагирование на кибератаки;
- исполнение федерального законодательства.

8.1.2 Обоснование необходимости реализации.

- законом №187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" установлена обязанность субъекта критической информационной инфраструктуры принимать организационные и технические меры для обеспечения безопасности значимых объектов критической информационной инфраструктуры;

- состав мер по обеспечению безопасности для значимого объекта соответствующей категории значимости утвержден приказом ФСТЭК России от 25 декабря 2017 г. N 239;

- среди обязательных мер – раздел XII. Реагирование на компьютерные инциденты:

- ИНЦ.1 Выявление компьютерных инцидентов;
- ИНЦ.2 Информирование о компьютерных инцидентах;
- ИНЦ.3 Анализ компьютерных инцидентов;
- ИНЦ.6 Хранение и защита информации о компьютерных инцидентах.

8.1.3 Обоснование возможности технической реализации.

- перечисленные выше задачи решаются с помощью системы менеджмента информации и событий безопасности (SIEM-системы);

- всё приобретаемое оборудование представлено на рынке продукции, поставляемой в регион, не относится к категории уникального оборудования, большинство видов оборудования или его аналоги ранее приобретались, имеется положительный опыт его эксплуатации;

- имеется опыт организации и осуществления закупок такого или аналогичного оборудования, опыт сотрудничества с широким кругом поставщиков;

- имеется персонал с соответствующим уровнем компетенции и опытом работы для организации эффективной эксплуатации закупаемого оборудования.

8.1.4 Принципы и порядок реализации.

- по состоянию на конец 2023 года в АО «Ульяновскэнерго» около 700 устройств (рабочих мест, серверов, сетевых устройств), которые необходимо контролировать;

- для реализации контроля в соответствии с требованиями приказа ФСТЭК России от 25 декабря 2017 г. №239 необходимо использовать систему менеджмента информации и событий безопасности (SIEM-систему);

- оборудование, преимущественно, там, где это возможно, приобретается с учётом стоимости лицензионного программного обеспечения (при необходимости), стоимости доставки и установки (настройки), других накладных расходов.

8.1.5 Предполагаемый эффект от реализации.

- выявление, анализ, хранение и защита информации об инцидентах;
- оперативное реагирование на кибератаки.

8.2 Приобретение программного комплекса выявления уязвимостей в информационных системах (Приказ ФСТЭК России от 18.02.2013 г. №21).

8.2.1 Цели реализации.

- автоматизированный поиск уязвимостей на рабочих станциях, серверах, сетевом оборудовании;
- обеспечение безопасности персональных данных при их обработке в информационных системах;
- исполнение федерального законодательства.

8.2.2 Обоснование необходимости реализации.

- законом №152-ФЗ "О персональных данных" установлена обязанность Оператора персональных данных принимать правовые, организационные и технические меры по обеспечению безопасности персональных данных;

- состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21;

- одна из обязательных мер - АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей;

- также подпункт «г» пункта 13 Постановления Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных

данных при их обработке в информационных системах персональных данных" требует применения сертифицированных средств защиты информации.

8.2.3 Обоснование возможности технической реализации.

- перечисленные выше задачи решаются с помощью средств анализа защищенности (сканеров уязвимостей);
- всё приобретаемое оборудование представлено на рынке продукции, поставляемой в регион, не относится к категории уникального оборудования, большинство видов оборудования или его аналоги ранее приобретались, имеется положительный опыт его эксплуатации;
- имеется опыт организации и осуществления закупок такого или аналогичного оборудования, опыт сотрудничества с широким кругом поставщиков;
- имеется персонал с соответствующим уровнем компетенции и опытом работы для организации эффективной эксплуатации закупаемого оборудования.

8.2.4 Принципы и порядок реализации.

- в 2023 году по договору №24/253/2023 от 07.08.2023 с ООО «Лист Трейд» приобретено ПО XSpider на 512 рабочих мест с обновлением в течение 1 года;
- для исполнения требований приказа ФСТЭК России от 18.02.2013 г. №21 необходимо ежегодное продление лицензии;
- оборудование, преимущественно, там, где это возможно, приобретается с учётом стоимости лицензионного программного обеспечения (при необходимости), стоимости доставки и установки (настройки), других накладных расходов.

8.2.5 Предполагаемый эффект от реализации.

- автоматизированный поиск уязвимостей на рабочих станциях, серверах, сетевом оборудовании;
- обеспечение безопасности персональных данных при их обработке в информационных системах.

8.3 Приобретение программного комплекса защиты персональных данных (Федеральный закон от 27.07.2006 №152-ФЗ).

8.3.1 Цели реализации.

- обеспечение безопасности персональных данных и критической информационной инфраструктуры;
- исполнение федерального законодательства.

8.3.2 Обоснование необходимости реализации.

- законом №152-ФЗ "О персональных данных" установлена обязанность Оператора персональных данных принимать правовые, организационные и технические меры по обеспечению безопасности персональных данных;

- законом №187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" установлена обязанность субъекта критической информационной инфраструктуры принимать организационные и технические мер для обеспечения безопасности значимых объектов критической информационной инфраструктуры;

- к организационным мерам в том числе относится ведение документации: перечней, регламентов, инструкций.

8.3.3 Обоснование возможности технической реализации.

- перечисленные выше задачи решаются с помощью системы ведения документации по защите информации;

- всё приобретаемое оборудование представлено на рынке продукции, поставляемой в регион, не относится к категории уникального оборудования, большинство видов оборудования или его аналоги ранее приобретались, имеется положительный опыт его эксплуатации;

- имеется опыт организации и осуществления закупок такого или аналогичного оборудования, опыт сотрудничества с широким кругом поставщиков;

- имеется персонал с соответствующим уровнем компетенции и опытом работы для организации эффективной эксплуатации закупаемого оборудования.

8.3.4 Принципы и порядок реализации.

- АО «Ульяновскэнерго» является объектом КИИ, в связи с этим необходим переход с облачного решения АльфаДок на серверную платформу, которая включает в себя документацию по КИИ;

- оборудование, преимущественно, там, где это возможно, приобретается с учётом стоимости лицензионного программного обеспечения (при необходимости), стоимости доставки и установки (настройки), других накладных расходов.

8.3.5 Предполагаемый эффект от реализации.

- обеспечение безопасности персональных данных и критической информационной инфраструктуры.

- исполнение требований федерального законодательства.