АССОЦИАЦИЯ
ЛИГА СОДЕЙСТВИЯ
ОБОРОННЫМ
ПРЕДПРИЯТИЯМ

КОМИТЕТ
ПО КОМПЛЕКСНОМУ ОБЕСПЕЧЕНИЮ
БЕЗОПАСНОСТИ НА ОТЕЧЕСТВЕННЫХ
ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЯХ

# ПРОТОКОЛ

**заседания Рабочей Группы по информационной безопасности**
**Комитета по комплексному обеспечению безопасности**
**на отечественных промышленных предприятиях**

**на тему:** ***«Реализация приоритетных задач информационной безопасности крупных организаций и госкорпораций и оптимизация ресурсов в нынешних экономических условиях»***

г. Москва, Карамышевская наб., д.44, 8 этаж, 10 февраля 2021 г.
конференц-зал № 822, АО «ИНКОМА» 14.00

| № | Фамилия, имя, отчество | Место работы |
|---|---|---|
| 1. | ТИЩЕНКО Максим Владимирович | **Руководитель рабочей группы по информационной безопасности** Комитета по комплексному обеспечению безопасности на отечественных промышленных предприятиях Ассоциации «Лига содействия оборонным предприятиям», Управляющий директор по автоматизации процессов аудитов и контроля ПАО «Промсвязьбанк» |
| 2. | АББЯСОВ Артур Ринатович | Руководитель направления по работе с ключевыми заказчиками АО «ИнфоВотч» |
| 3. | АГЕЕВ Андрей Алексеевич | Координатор Рабочей группы по информационной безопасности Комитета по комплексному обеспечению безопасности на отечественных промышленных предприятиях, Директор по спецпроектам АО «ИНКОМА» |
| 4. | АНДРЕЕВ Сергей Викторович | Начальник отдела внутреннего контроля АО «Корпорация «Комета» |
| 5. | БОЛОТИН Евгений Юрьевич | Руководитель Департамента информационной безопасности АО «Объединенная двигателестроительная корпорация» |
| 6. | ВАСИЛЬЕВ Алексей Николаевич | Заместитель генерального директора ФГУП «Российские сети вещания и оповещения» (ФГУП «РСВО») |
| 7. | ВИХОРЕВ Виктор Сергеевич | Директор по информационной безопасности ООО «РТ-Информ» |
| 8. | ВОРОБЬЕВ Евгений Германович | Заведующий кафедрой информационной безопасности Факультета компьютерных технологий и информатики ФГАОУ ВО «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), к.т.н., доцент |
| 9. | ГОЛОВКИН Денис Викторович | Заместитель руководителя Рабочей Группы по информационной безопасности, Директор по спецпроектам ООО «Код Безопасности» |
| 10. | ЗЕРНОВ Алексей Александрович | Главный специалист Департамента экономической и информационной безопасности АО «НПО «Высокоточные комплексы» |
| 11. | ЗУБАРЕВ Николай Вадимович | Директор по направлению «Информационная безопасность» АНО «Цифровая экономика» |
| 12. | КАЛАШНЕВ Сергей Викторович | Ответственный секретарь Комитета по комплексному обеспечению безопасности на отечественных промышленных предприятиях, Ведущий специалист АО «РТ-Охрана» |

| | | |
|---|---|---|
| 13. | КАЛЕНСКИЙ<br>Назар Александрович | Главный специалист ООО «НИЦ ТСО» (Холдинг «СИБЕР») |
| 14. | КОМИССАРОВ<br>Александр Геннадьевич | Президент Ассоциации содействия выполнения государственного оборонного заказа |
| 15. | КРЫЛОВ<br>Александр Аркадьевич | Проректор по внешним коммуникациям ФГАОУ ВО «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина) |
| 16. | КУЗЬМИН<br>Олег Николаевич | Заместитель директора департамента ИТ и связи по информационной безопасности АО «Концерн ВКО «Алмаз-Антей» |
| 17. | ЛАВРЕНКО<br>Александр Александрович | Начальник управления информационной безопасности ФГУП «Российские сети вещания и оповещения» (ФГУП «РСВО») |
| 18. | ЛИСОВИК<br>Сергей Валериевич | Директор по информационной безопасности АО «ИНКОМА» |
| 19. | МАКОСКО<br>Андрей Александрович | Руководитель Службы информационной безопасности АО АКБ «НОВИКОМБАНК» |
| 20. | НИКОЛАЕВА<br>Анастасия Всеволодовна | Директор по развитию бизнес-решений и маркетингу АО «ИНКОМА» |
| 21. | ОРЕХОВ<br>Вилионор Александрович | Начальник отдела информационной безопасности АО «Объединенная судостроительная корпорация» |
| 22. | ОРЛОВ<br>Алексей Александрович | Руководитель направления Службы информационной безопасности АО АКБ «НОВИКОМБАНК» |
| 23. | ПЕРЕДНЯ<br>Вячеслав Александрович | Начальник бюро по информационной безопасности АО «Корпорация «Комета» |
| 24. | ПЛЯСУНОВ<br>Сергей Сергеевич | Главный конструктор ФГУП «Российские сети вещания и оповещения» (ФГУП «РСВО») |
| 25. | РОДНИКОВ<br>Станислав Львович | Директор по развитию направления «Безопасный город» АО «ОПК» |
| 26. | САТАРОВ<br>Владислав Александрович | Директор по стратегическому развитию информационных ресурсов, руководитель блока «Умный и Безопасный Город» АО «ИНКОМА» |
| 27. | СЕМЕСЬКО<br>Юлия Владимировна | Генеральный директор АО «ИНКОМА» |
| 28. | СТАВРО<br>Дмитрий Владиславович | Руководитель проектов АО «ИНКОМА» |
| 29. | СТОРОЖУК<br>Артём Андреевич | Ответственный секретарь Рабочей группы по информационной безопасности Комитета по комплексному обеспечению безопасности на отечественных промышленных предприятиях, помощник Члена Бюро Ассоциации «Лига содействия оборонным предприятиям», генерального директора АО «РТ-Пожарная безопасность» |
| 30. | СУБОЧ<br>Михаил Семенович | Вице-президент Ассоциации содействия выполнения государственного оборонного заказа |
| 31. | ФОМИЧЕВ<br>Павел Александрович | Начальник управления ИТ - Заместитель директора департамента Информационных технологий и обеспечения безопасности ООО «Группа ПОЛИПЛАСТИК» |
| 32. | ЮРШЕВ<br>Андрей Юрьевич | Ведущий эксперт АО «ИнфоВотч» |

АССОЦИАЦИЯ ЛИГА СОДЕЙСТВИЯ ОБОРОННЫМ ПРЕДПРИЯТИЯМ

РАБОЧАЯ ГРУППА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМИТЕТА ПО КОМПЛЕКСНОМУ ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ НА ОТЕЧЕСТВЕННЫХ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЯХ

**ПОВЕСТКА**

**заседания Рабочей Группы по информационной безопасности Комитета по комплексному обеспечению безопасности на отечественных промышленных предприятиях**

**на тему: *«Реализация приоритетных задач информационной безопасности крупных организаций и госкорпораций и оптимизация ресурсов в нынешних экономических условиях»***

г. Москва, Карамышевская наб., д.44, 8 этаж, конференц-зал № 822, АО «ИНКОМА»

10 февраля 2021 года
14:00

**Вступительное слово *Тищенко Максима Владимировича***, *Руководителя рабочей группы по информационной безопасности, Управляющего директора по автоматизации процессов аудита и контроля ПАО «Промсвязьбанк».*

1. «Формирование единой политики информационной безопасности для предприятий оборонно-промышленного комплекса Российской Федерации».

**Докладчик – *Кузьмин Олег Николаевич***, *Заместитель директора департамента ИТ и связи по информационной безопасности АО «Концерн ВКО «Алмаз-Антей».*

**Содокладчик – *Макоско Андрей Александрович***, *Руководитель Службы информационной безопасности АО АКБ «НОВИКОМБАНК».*

2. «Актуальные проблемы информационной безопасности в современных экономических условиях. Возможные решения и пути развития».

**Докладчик – *Воробьев Евгений Германович***, *Заведующий кафедрой информационной безопасности Факультета компьютерных технологий и информатики ФГАОУ ВО «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), д.т.н., доцент.*

3. «Вопросы взаимодействия со ФСТЭК России по категорированию КИИ».

**Докладчик – *Головкин Денис Викторович***, *Заместитель руководителя Рабочей Группы по информационной безопасности, Директор по спецпроектам ООО «КОД БЕЗОПАСНОСТИ».*

**Содокладчик – *Юршев Андрей Юрьевич***, *Ведущий эксперт АО «ИнфоВотч».*

4. «Импортозамещение в информационной безопасности».

**Докладчик – *Лисовик Сергей Валериевич***, *Директор по информационной безопасности АО «ИНКОМА».*

5. Дискуссия.

**Заключительное слово**, ***Тищенко Максима Владимировича***, *Руководителя рабочей группы по информационной безопасности, Управляющего директора по автоматизации процессов аудита и контроля ПАО «Промсвязьбанк».*

***

Вступительное слово **Тищенко Максима Владимировича**, Руководителя рабочей группы по информационной безопасности Комитета по комплексному обеспечению безопасности на отечественных промышленных предприятиях Ассоциации «Лига содействия оборонным предприятиям», Управляющего директора по автоматизации процессов аудитов и контроля ПАО «Промсвязьбанк».

**М.В. Тищенко** поблагодарил всех присутствовавших участников за активное включение в работу экспертной группы, отметив почти 100% явку членов рабочей группы.

***

С докладом на тему: «О формировании единой политики информационной безопасности для предприятий оборонно-промышленного комплекса Российской Федерации» выступил **Кузьмин Олег Николаевич**, Заместитель директора департамента ИТ и связи по информационной безопасности АО «Концерн ВКО «Алмаз-Антей», выделив на первый план внедрение на предприятиях ОПК технологий цифрового производства. «Задачами цифровизации производства являются задачи создания и внедрения на предприятии современных интегрированных информационных систем и передовых производственных технологий, цифровых фабрик, охватывающих все бизнес-процессы и подразделения предприятия, а также все стадии жизненного цикла производимых изделий».

Цифровая трансформация позволит решать на новом уровне непрерывно усложняющиеся задачи, стоящие перед промышленными предприятиями.

***

Докладчик – **Макоско Андрей Александрович**, Руководитель Службы информационной безопасности АО АКБ «НОВИКОМБАНК».

В своем содокладе **А.А. Макоско** рассказал об актуальных источниках угроз ИБ, целях развития системы обеспечения ИБ, путях построения системы ИБ на предприятии, привел примеры организационных и технических мероприятий по обеспечению ИБ, иерархии документов в области ИБ, о Стандартах в области ИБ.

***

Докладчик – **Воробьев Евгений Германович**, Заведующий кафедрой информационной безопасности Факультета компьютерных технологий и информатики ФГАОУ ВО «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), д.т.н., доцент.

В своем докладе **Е.Г. Воробьев** выделил актуальные проблемы информационной безопасности в современных экономических условиях, а также обозначил возможные решения и пути развития, отметив что имеется проблема безопасности цифрового производства и цифровой экономики, а именно: универсальность сетевых протоколов сети Интернет и принципов удаленного управления распределенными системами позволяет транзитивно замкнуть все управляющие системы производственной, финансовой и общественно-политической сферы в единое киберпространство; глобальная доступность киберфизических объектов порождает проблему обеспечения устойчивой работы цифрового производства в условиях случайных и целенаправленных компьютерных атак, приводящих к долговременному и трудно обнаруживаемому воздействию на управление технологическими процессами, что может повлечь катастрофические последствия.

Существуют требования к новым нормативным документам ФСТЭК, которые существенно увеличивают трудоемкость сертификационных исследований:

1. Методика выявления уязвимостей и не декларированных возможностей утверждена ФСТЭК России 11 февраля 2019 г., применяется при проведении сертификационных испытаний с 1 мая 2019.

2. «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (Требования к уровням доверия)» утверждены приказом ФСТЭК России от 30 июля 2018 г. No 131, приказ зарегистрирован Минюстом России 14 ноября 2018 г. No 52686, вступил в силу с 1 августа 2018 г., применяется при проведении сертификационных испытаний с 1 мая 2019 г.

**Е.Г. Воробьев** особое внимание уделил подготовке специалистов по ИБ. Так называемый практико-ориентированный подход к подготовке специалистов по ИБ. Цель данного подхода – приведение содержания и результативности образовательных программ в соответствие с современным уровнем технологической инфраструктуры и ожиданиями ведущих работодателей. Современный специалист по ИБ должен владеть методами решения следующих задач: обнаружение и анализ киберугроз, направленных на нарушение киберустойчивости систем цифрового производства и цифровой экономики, робототехнический систем; реализация адаптивной активной системы предотвращения киберугроз с использованием методов искусственного интеллекта для управления параметрами и архитектурой защищенной системы; разработка методов безопасной обработки больших и сверхбольших массивов данных с использованием гомоморфной криптографии, создание глобальной доверенной среды с использованием блокчейн и оптимизация информационных потоков на основе BigData; разработка систем мониторинга, оценки состояния, расследования инцидентов кибербезопасности и киберустойчивости для прогнозного управления безопасностью цифрового пространства.

Для отработки практических навыков специалистов, экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий, а также для тестирования программного и аппаратного обеспечения путем моделирования компьютерных атак и отработки реакций на них будет использоваться киберполигон.

***

Докладчик – **Головкин Денис Викторович**, Заместитель руководителя Рабочей Группы по информационной безопасности, Директор по спецпроектам ООО «КОД БЕЗОПАСНОСТИ».

В своем докладе **Д.В. Головкин** остановился на тех вопросах, которые необходимо сформировать для организации консолидированной позиции с представителями регулятора ФСТЭК России, отметив, что большая часть вопросов связана с категорированием КИИ. Так же необходимость принятия в действие существующего проекта Методики моделирования угроз безопасности информации ФСТЭК и создания ФСТЭК типовых рекомендаций по определению объектов КИИ.

***

Содокладчик – **Юршев Андрей Юрьевич**, Ведущий эксперт АО «ИнфоВотч».

В своем выступлении **А.Ю. Юршев** остановился на вопросах, возникающих при категорировании объектов КИИ, в том числе определении границ объектов КИИ, расчета значений отдельных показателей.

***

Докладчик – **Лисовик Сергей Валериевич**, Директор по информационной безопасности АО «ИНКОМА».

В своем докладе **С.В. Лисовик** уделил особое внимание проблемам, связанным с использованием серверного программного обеспечения иностранного производства в секторе КИИ. «В наше время сложно представить эффективный бизнес-процесс без его комплексной автоматизации и использования различных программных продуктов и информационных систем. Серверное программное обеспечение это фундамент. От драйверов устройств и операционных систем, до веб серверов и гипервизоров. Вся эта цифровая экосистема с ее бесконечным многообразием жизненно необходима для функционирования нашей экономики, оборонной промышленности и прочих сфер деятельности» - добавил эксперт.

«Большинство аттестованных систем построено на базе иностранного серверного ПО, имеющего уже сейчас Российские аналоги. В центрах обработки данных используются иностранные гипервизоры, среды оркестровки и автоматизации, системы хранения и резервного копирования данных. Разрабатываемые в рамках государственных контрактов информационные системы функционируют под управлением недоверенных программных продуктов. Все это абсолютно точно ставит под угрозу само понятие безопасности информации и государства в целом. Средства и системы защиты помогают нам добиться соблюдения режима конфиденциальности, предотвращают утечки, позволяют изолировать периметр информационной системы, но эффективность всего этого с учетом вышесказанного вызывает лично у меня большие сомнения. Ценность конфиденциальности заключается в возможности предоставления упорядоченного и регламентированного доступа к данным. Но все это имеет смысл лишь когда есть сами данные, когда есть что защищать и есть что терять.

Говоря о Российских аналогах, руководствуюсь исключительно личным опытом внедрения и проектирования информационных систем. В своей практике я сталкивался с функционирующими ЦОДами под управлением систем виртуализации и хранения данных Российского производства. Участвовал в разработке информационных систем, ориентированных на применение в своем составе программных модулей с открытым исходным кодом. Принимал участие в проектах, направленных на внедрение Российских ОС в пользовательском сегменте (АРМ). И могу вам сказать, что это работает и работает по сей день, и работает хорошо.

Мы с вами живем во время цифровых трансформаций. Каждому известному вам примеру научного термина сейчас соответствует его цифровой двойник. Цифровое пространство, цифровое государство, цифровая экономика, цифровая граница, цифровой экстремизм. И если хакерская атака с целью похитить данные кредитной карты в масштабах государства выглядит как банальная квартирная кража со взломом, то уничтожение информации отдельно взятого субъекта КИИ без возможности ее восстановления сравнимо со взрывом атомной бомбы. Говоря об информационной безопасности и защите данных, мы привыкли думать, что злоумышленник стоит у ворот, но используя иностранное ПО, мы сами приглашаем его внутрь. В электронное сердце нашего цифрового отечества».

В качестве мер противодействия **С.В. Лисовик** предложил участникам рабочей группы:

1. рассмотреть возможность создания типового технического задания на разработку новых ИС внутри Ассоциации «Лига содействия оборонным предприятиям», исключающего наличие иностранного ПО;
2. инициировать комплекс мероприятий, направленный на сбор информации с целью оценки возможности переноса существующих ИС, операторами которых

являются участники Ассоциации «Лига содействия оборонным предприятиям» на Российское серверное ПО.

***

В своем заключительном слове руководитель Рабочей группы **М.В. Тищенко** высказал мнение о том, что совместными усилиями необходимо самореализовываться в сфере информационной безопасности, повышать свой уровень зрелости и компетенций.

Экспертами была предложена и поддержана идея создать и провести в формате ВКС вебинар на площадке Рабочей группы и Комитета по комплексному обеспечению безопасности на отечественных промышленных предприятиях Ассоциации «Лига содействия оборонным предприятиям» с использованием российской коммуникационной платформы для специалистов информационной безопасности разных уровней зрелости в целях повышения компетенций и получения новых знаний в области информационной безопасности.

По итогу заседания сформированы предложения в адрес ФСТЭК России, а также предложения в части категорирования КИИ и внесения изменений в проект единой политики ИБ.

***

По результатам заседания принято следующее **РЕШЕНИЕ**:

I. Принять к сведению информацию, изложенную в докладах:

- **Тищенко Максима Владимировича**, Руководителя рабочей группы по информационной безопасности Комитета по комплексному обеспечению безопасности на отечественных промышленных предприятиях Ассоциации «Лига содействия оборонным предприятиям», Управляющего директора по автоматизации процессов аудитов и контроля ПАО «Промсвязьбанк»;

- **Кузьмина Олега Николаевича**, Заместителя директора департамента ИТ и связи по информационной безопасности АО «Концерн ВКО «Алмаз-Антей»;

- **Макоско Андрея Александровича**, Руководителя Службы информационной безопасности АО АКБ «НОВИКОМБАНК»;

- **Воробьева Евгения Германовича**, Заведующего кафедрой информационной безопасности Факультета компьютерных технологий и информатики ФГАОУ ВО «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), д.т.н., доцента;

- **Головкина Дениса Викторовича**, Заместителя руководителя Рабочей Группы по информационной безопасности, Директора по спецпроектам ООО «КОД БЕЗОПАСНОСТИ»;

- **Юршева Андрея Юрьевича**, Ведущего эксперта АО «ИнфоВотч»;

- **Лисовика Сергея Валериевича**, Директора по информационной безопасности АО «ИНКОМА».

II. Подготовить перечень инициатив нормативно-правовых актов регламентирующих КИИ.

**Ответственный:** аппарат Рабочей группы по ИБ.

**Срок:** 28 февраля 2021 года.

III. Подготовить письмо в адрес руководителей предприятий, входящих в Союз машиностроителей России и Ассоциацию «Лига содействия оборонным предприятиям» с информацией о проведении образовательного вебинара для специалистов информационной безопасности.
**Ответственный:** аппарат Рабочей группы по ИБ.
**Срок:** 28 февраля 2021 года.

IV. Подготовить письмо в адрес руководства Ассоциации «Лига содействия оборонным предприятиям» с просьбой оказать информационную поддержку проведения образовательного вебинара.
**Ответственный:** аппарат Рабочей группы по ИБ.
**Срок:** 28 февраля 2021 года.

V. Поручить **Кузьмину Олегу Николаевичу**, Заместителю директора департамента ИТ и связи по информационной безопасности АО «Концерн ВКО «Алмаз-Антей» организовать образовательный курс для специалистов ИБ в рамках работы экспертной группы.
**Ответственный:** Кузьмин О.Н.
**Срок:** 31 марта 2021 года.

**Руководитель рабочей группы по информационной безопасности Комитета по комплексному обеспечению безопасности на отечественных промышленных предприятиях Ассоциации «Лига содействия оборонным предприятиям», Управляющий директор по автоматизации процессов аудитов и контроля ПАО «Промсвязьбанк»** **М.В. Тищенко**