МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИРЭА – Российский технологический университет»
РТУ МИРЭА

ИКБ направление «Кибербразведка и противодействие угрозам с применением технологий искусственного интеллекта» 10.04.01

Кафедра КБ-4 «Интеллектуальные системы информационной безопасности»

Практическая работа

по дисциплине
«Управление информационной безопасностью»

Группа:
ББМО-01-22
Выполнила:
Огольцова Н.Д.

Проверил:
Пимонов Р.В.

Москва 2023

УТВЕРЖДАЮ

Учредитель ООО «Вкусно и Ладно»

_____/_____ /

«___» _____ 20__г.

ПЛАН
РЕАГИРОВАНИЯ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ В КОМПАНИИ

ООО «Вкусно и Ладно»

1 Общие положения

1.1 Назначение Плана

Настоящий План реагирования на компьютерные инциденты в ООО «Вкусно и Ладно» предназначен для формирования обоснованных организационных требований к составу и содержанию мероприятий по обеспечению реагирования на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак.

1.2 Нормативно-правовые акты, методические документы, используемые для оценки угроз безопасности информации и разработки Плана

Настоящий План составлен в соответствии со следующими действующими нормативно-методическими документами по защите информации:

– Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных»;

– Приказ Федеральной службы безопасности Российской Федерации от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации»;

– Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденное приказом ФСБ России от 09.02.2005 года № 66 (зарегистрирован Минюстом России 03.03.2005, регистрационный № 6382)

– Методические рекомендации по разработке плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации;

– Приказ ФСБ России от 24.07.2018 года № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах и Порядка получения субъектами КИИ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»;

– Постановление Правительства РФ "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" от 01.11.2012 года № 1119.

– Постановление Правительства РФ от 17.02.2018 года№162 "Об утверждении Правил осуществления госконтроля в области обеспечения безопасности значимых объектов КИИ РФ".

2 Технические характеристики и состав КИ

Наименование систем и сетей, для которых разработан План:

– объект 1 – информационная система персональных данных «Вкусно и Ладно»;

– объект 2 – ЛВС, в рамках которой работники обеспечивают обмен информацией;

– объект 3 – сервер, на котором хранятся БД ИСПДн, «Вкусно и Ладно».

В Таблице 1 описана информация о технических характеристиках.

Таблица 1 – Технические характеристики и состав ЗООКИ

Описание сведений	**Номер объекта**	**Технические характеристики и состав**
Взаимодействие КИ и сетей электросвязи	Объекты 1, 2, 3	Все объекты взаимодействую с сетями электросвязи. Они

		обеспечивают передачу данных между всеми объектами. Характеристики и состав объектов подробнее описаны в документе «Модель угроз безопасности информации». Взаимосвязь между объектами происходит для обмена информацией внутри организации, а также для предоставления и оказания услуг.
Программные и программно-аппаратные средства	Объекты 1, 3	Техническое описание средств входящие в группу «Объект 1» и «Объект 2»: - DELL T630 16SFF 2xE5-2603v3 32GB, ОС: Astra Linux. 4 ядра. Оперативная память 12 ГБ, объем жесткого диска 1024 ГБ. Встроенные общесистемные прикладные средства, сертификация и экспертиза средств информации не производилась.
Наличие средств архивирования и резервного копирования данных	Отсутствуют	Отсутствуют
Подключение КИ к корпоративному (ведомственному) центру ГосСОПКА	Отсутствуют	Отсутствуют

Установленные на КИ средства ГосСОПКА	Отсутствуют	Отсутствуют

3 События (условия), при наступлении которых начинается реализация предусмотренных Планом мероприятий

В данном разделе определяется список событий (условий), при наступлении которых начинается реализация защитных действии предусмотренных Планом:

1) Прекращение работы АРМ, сервисов и иных компонентов ЗОКИИ;
2) Нарушение установленного в организации режима доступа к информации или компонентам ЗОКИИ;
3) Функционирование ВПО;
4) Компрометация данных и утеки данных;
5) Вредоносное программное обеспечение (или код);
6) Несанкционированный (нелегитимный) доступ в систему;
7) Сбор сведений о внешних или внутренних ресурсах;
8) Несанкционированное изменение информации на элементах ЗОКИИ;
9) Атаки с использованием социальной инженерии;
10) Нарушение работы инфраструктуры или контролируемого ресурса;
11) Наличие уязвимостей в контролируемом ресурсе;
12) Иные нарушения в работе элементов ЗОКИИ, вызывающих прекращение выполнения его целевых функций

4 Мероприятия, проводимые в ходе реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак, а также время, отводимое на их реализацию.

В Таблице 2 описана информация о мероприятиях, которые будут проводиться в ходе реагирования на компьютерные инциденты КИ ООО «Вкусно и Ладно». Также отражены меры по ликвидации последствий и отводимое на их реализацию время.

Таблица 2 – Меры по ликвидации последствий от компьютерных атак

Наименование события (условия)	**Организационные/ технические меры**	**Подразделения или должностные лица, ответственные за проведение мероприятий**	**Время на реализацию мероприятия**
Уничтожение или повреждение данных	Обучение персонала. Ограниченный доступ к конфиденциальной информации. Выполнение всех требований законодательства по защите персональных данных.	Руководители отдела ИБ, IT-отдел, SOC	Обучение новых сотрудников 3 месяца. Остальные этапы: бессрочно.
Компрометация данных и утеки данных			

Вредоносное программное обеспечение (или код)	Обучение персонала. Ограниченный доступ персонала к ресурсам (как физическое, так и прав в сети). Использование сертифицированного программного обеспечения для обнаружения вредоносного ПО (антивирусы). Мониторинг сетевых портов. Ведение журналов событий. Обнаружение вторжений. Ликвидация последствий и быстрое реагирование на инциденты. Изоляция зараженных систем от остальных ресурсов. Ликвидация угрозы на зараженных системах.	Руководители отдела ИБ, IT-отдел, SOC	Обучение новых сотрудников 3 месяца. Этапы обнаружения проводятся постоянно. Время: 40 минут.
Несанкционированный (нелегитимный) доступ в систему	Обучение персонала. Ограниченный доступ персонала к ресурсам (как физическое, так и прав в сети). Регулярное обновление всего программного обеспечения и автоматическое включение обновлений безопасности. Проведение аутентификации пользователей. Соблюдение парольной политики. Использование сертифицированного программного обеспечения для обнаружения вредоносного ПО (антивирусы). Мониторинг сетевых портов. Ведение журналов событий. Использование систем DLP и CASB. Обнаружение вторжений (Secret Net Studio).	Руководители отдела ИБ, IT-отдел, SOC	Обучение новых сотрудников 3 месяца. Этапы обнаружения проводятся постоянно. Время: 40 минут.

	Ликвидация последствий и быстрое реагирование на инциденты. Изоляция скомпрометированных систем от остальных ресурсов. Ликвидация доступа злоумышленника в системах.		
Сбор сведений о внешних или внутренних ресурсах	Обучение персонала. Правильная настройка открытых портов. Выполнение всех требований законодательства по защите персональных данных. Использование сертифицированного программного обеспечения для обнаружения вредоносного ПО (антивирусы). Мониторинг сетевых портов. Ведение журналов событий. Обнаружение вторжений (Secret Net Studio). Ликвидация последствий и быстрое реагирование на инциденты. Изоляция скомпрометированных систем от остальных ресурсов. Ликвидация доступа злоумышленника в системах.	Руководители отдела ИБ, IT-отдел, SOC	Обучение новых сотрудников 3 месяца. Этапы обнаружения проводятся постоянно. Время: 40 минут.
Атаки с использованием социальной инженерии	Обучение персонала. Проведение тренингов и проверок сотрудников. Использование многофакторной аутентификации. Разработка и поддержка политики безопасности.	Руководители отдела ИБ, IT-отдел, SOC	Обучение новых сотрудников 3 месяца. Тренинги и проверка сотрудников должна проводиться

			ежеквартально (4 раза в год).
Нарушение работы инфраструктуры или контролируемого ресурса	Ограниченный доступ персонала к ресурсам (как физическое, так и прав в сети). Обучение персонала. Использование сертифицированного программного обеспечения для обнаружения вредоносного ПО (антивирусы). Мониторинг сетевых портов. Ведение журналов событий. Обнаружение вторжений (Secret Net Studio). Ликвидация последствий и быстрое реагирование на инциденты. Изоляция скомпрометированных систем от остальных ресурсов. Ликвидация доступа злоумышленника в системах.	Руководители отдела ИБ, IT-отдел, SOC	Обучение новых сотрудников 3 месяца. Этапы обнаружения проводятся постоянно. Время: 40 минут.
Наличие уязвимостей в контролируемом ресурсе	Ограниченный доступ персонала к ресурсам (как физическое, так и прав в сети). Обучение персонала. Использование сертифицированного программного обеспечения для обнаружения вредоносного ПО (антивирусы). Мониторинг сетевых портов. Ведение журналов событий. Обнаружение вторжений (Secret Net Studio). Ликвидация последствий и быстрое реагирование на инциденты.	Руководители отдела ИБ, IT-отдел, SOC	Обучение новых сотрудников 3 месяца. Этапы обнаружения проводятся постоянно. Время: 40 минут.

5 Подразделения и должностные лица, ответственные за проведение мероприятий по реагированию на КИ и принятие мер по ликвидации последствий КА

В Таблице 3 описана информация о должностных лицах и подразделениях, которые отвечают за принятие мер и ликвидацию последствий КА.

Таблица 3 – Подразделения и должностные лица

Должность	ФИО сотрудника	Роль	Контакты	Реквизиты приказа
Руководитель отдела ИБ	Ховрин Максим Максимович	Курирует деятельность по обеспечению ИБ Принимает решение о привлечении подразделений и должностных лиц ФСБ России к проведению мероприятий по реагированию на КИ	+79159151414 hovrinmm@vkuusno.ru	Приказ (распоряжение) от 14.02.2023 № 123

Специалист по защите информации	Кружок Андрей Юрьевич	Проводит предварительную проверку состояния ИБ ЗОКИИ; Участвует в мероприятиях по реагированию КИ ЗОКИИ;	+79149151515 kruzokau@vkuusno.ru	Приказ (распоряжение) от 14.02.2023 № 123
Специалист администрирования SOC	Треугольник Степан Степанович	Эксплуатирует и администрирует ЗОКИИ; Участвует в мероприятиях по выявлению, реагированию и расследованию КИ ЗОКИИ.	+79119111415 treygolnikss@vkuusno.ru	Приказ (распоряжение) от 14.02.2023 № 123

6 Условия привлечения подразделений и должностных лиц ФСБ России.

Условия привлечения подразделений и должностных лиц ФСБ России:

– лицо (работник) или должностные лица, ответственные за обеспечение безопасности КИ не справляются с ликвидацией компьютерного инцидента;

– КИ привёл к прекращению функционирования ЗОКИИ;

– компьютерный инцидент привел к последствиям, которые не представляется возможным предотвратить должностными лицами организации.

7 Порядок проведения мероприятий по реагированию на КИ и принятию мер по ликвидации последствий КА в отношении КИ совместно с привлекаемыми подразделениями и должностными лицами ФСБ России

Порядок проведения мероприятий по реагированию на КИ и принятию мер по ликвидации последствий КА в отношении КИ совместно с привлекаемыми подразделениями и должностными лицами ФСБ России:

1. Определение значимого объекта критической информационной инфраструктуры и его функционирования.

2. Разработка и утверждение руководителем организации регламента информирования ФСБ России о компьютерных инцидентах.

3. Проведение предварительных испытаний в соответствии с программой и методикой предварительных испытаний.

4. Актуализация модели угроз безопасности и документации технического проекта.

5. Незамедлительное информирование ФСБ о всех компьютерных инцидентах через Национальный координационный центр по компьютерным инцидентам.