МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(дипломная работа)

На тему «Разработка стенда для моделирования реакции распределенной информационной системы на компьютерные атаки»

Исполнитель Покатаев Владимир Дмитриевич
(фамилия,имя,отчество)

Руководитель Грызунов Виталий Владимирович
(фамилия, имя, отчество)

«К защите допускаю»

Заведующий кафедрой_____

(подпись)

_____
(ученаястепень,ученое звание)

Бурлов В.Г.
(фамилия,имя,отчество)

«» 20г

Санкт–Петербург

2023

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В современном обществе огромную роль играют объекты критической информационной инфраструктуры (КИИ). КИИ - это совокупность информационных систем и телекоммуникационных сетей, имеющих решающее значение для функционирования ключевых сфер национальной и общественной жизни: здравоохранения, промышленности, связи, транспорта, энергетики, финансового сектора, экономики государств и регионов.

Эти объекты с недавнего времени перестали быть только государственными, сейчас объектом КИИ может быть, как крупная компания, так и индивидуальный предприниматель. С нарушением деятельности КИИ может быть связано большое количество проблем как у государства, так и общества, за счет тех процессов что они выполняют. С текущими темпами цифровизации такие объекты стали оснащаться большим количеством прогрессивных информационных систем, что сделало их работу существенно быстрее, но также создало огромный плацдарм для различного рода хакерских атак.

На безопасность объектов критической информационной инфраструктуры выделяются большие бюджеты. Для снижения риска при атаках них. Но остается актуальным вопрос, как же эффективней оценивать применяемые меры по противодействию деструктивным воздействиям со стороны хакеров.

Данная совокупность факторов определяет актуальность настоящей ВКР, целью которой является повышение достоверности оценивания экспертом рассматриваемой системы при помощи стенда.

Цель дипломной работы:

Повысить достоверность оценивания системы экспертом.

Задачи необходимые для достижения цели:

- Составить описание компании с точки зрения ИБ
- Рассмотрение наиболее распространенных компьютерных вирусов;

- Анализ наиболее актуальных векторов атак;
- Моделирование стенда для реакции РИС;
- Собрать статистические данные от специалистов в сфере информационной безопасности;
- Проанализировать полученные данные на предмет согласованности при различных условиях.

ГЛАВА 1. ОПИСАНИЕ ОБЪЕКТА ЗАЩИТЫ НА ПРИМЕРЕ КОМПАНИИ MOBILEYE

1.1 Описание объекта КИИ

Обеспечение безопасности КИ, всегда считалась ключевой проблемой безопасности государств и частных организаций. КИИ относится к ключевой инфраструктуре, которая используется для предоставления основных услуг, таких как транспорт, связь, энергетика, здравоохранение и финансы. По мере того как частные компании развиваются, все больше их роль становится более весомой в жизни обычных людей.

Крупные корпорации по масштабам своих предприятий уже могут сравниться с государственными. Их широкая интеграция в общество и нарастающая сложность внутренних процессов и технологий создают большое поле для проявления различных видов уязвимостей, закрытие которых является первостепенной задачей перед любым отделом безопасности.

1.1.1 Рассмотрение объекта защиты

В виде объекта для изучения свойств, угроз и мер защиты КИИ, предлагаю в данной работе обратить внимание на компанию Mobileye. Данная корпорация начала свое существование в 1999 году и существует по сегодняшний день, являясь дочерней компанией Intel. Эта компания специализируется на разработке развитых систем помощи водителю, предназначенных для снижения опасности при вождении и увеличении скорости реагирования на инциденты во время движения, так же компания поставляет значительную часть своего оборудования государственным организациям, для обеспечения безопасности при вождении общественного транспорта, а также коммерческих грузовых перевозок.

В случае нарушения деятельности компании может пострадать большое количество людей, так как неправильная работа в связи с нарушением цифровой

инфраструктуры компании может сказаться на средства контроля автомобилей на дорогах и может привести к большому числу аварий. Так же можно сказать, что если будет затронута большая часть организации, то ущерб понесенный в следствии атак на информационную систему, может выйти за пределы одной страны, а учитывая масштабы компании, это может коснуться далеко не одного государства. Что так же в свою очередь прибавляет значимость к защите объектов такого рода.

Размеры этой корпорации и ее значимость для общества дают ей право претендовать на объект КИИ в сфере транспорта. Так же есть и другие признаки, такие как:

Развитые ИС – информационные системы, содержащие базы данных и обеспечивающие ее обработку информационных технологий и технических средств

Наличие ИТС – информационно технологической системы, предназначенной для передачи по линиям связи информации, к которой осуществляется доступ с использованием ИС.

АСУ – комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами.

Большая социальная значимость, так как системами компании пользуются не только частные организации, а также государственные, в сфере общественного транспорта и грузовых перевозок. Исходя из перечисленных пунктов, можно предварительно отнести компанию Mobileye к социально значимым объектам, что в свою очередь дает называть ее объектом критической информационной инфраструктуры.

Далее будут рассмотрены типовые угрозы, свойственные этой компании, произведен разбор по всем аспектам информационной безопасности, что поможет более точно определить наиболее слабые места в структуре такой

крупно организации. И поможет далее рассмотреть их подробнее с точки зрения современного законодательства.

1.1.2 Возможные векторы атак

Необходимость эффективной защиты организации становится очевидной стратегией для компаний. Однако существует множество нюансов, поскольку для защиты КИИ нужно учитывать различные переменные.

Во-первых, в связи с растущей взаимосвязью различных сетевых устройств, важно применять комплексные средства защиты, которые помогут обеспечить контроль над всей сетью, вне зависимости от ее масштабов [6].

Во-вторых, нельзя оставлять без внимания человеческий фактор. Очень важно проводить тематические беседы с коллективом на тему важности информационной безопасности, и угрозы, которые можно понести при ее несоблюдении.

Таблица 1 - Описание объекта защиты, анализ потенциально уязвимых мест.

	Целостность	Доступность	Конфиденциальность	Согласованность	Аутентичность
Программный	Программу нельзя изменить, имеет контрольную сумму.	Доступ к программе существляется через ЭВМ.	С программами работают только те пользователи, у которых есть доступ.	Программы аттестованы регулятором.	Программа работает без ошибок и артефактов.
Аппаратный	За оборудованием идет контроль со стороны службы охраны.	К оборудованию имеется.	К аппаратной части (сервера/автоматизированные системы) имеют доступ только сотрудники с допуском.	Непротиворечивость компонентов задействованных в системе.	Качество оборудования соответствует требованиям.

Персонал	Сотрудник не покинет систему, пока с ним подписан контракт.	Возможность найти сотрудника как на работе, так и в не рабочее время. Изъятие загран паспорта.	Уровни допуска персонала.	Непротиворечивость действий сотрудника с системой и персоналом.	Достоверность и подлинность выполненной им работы.
Обеспечивающий	Правовая база является устойчивой и не подлежит кардинальной изменчивости.	К документам имеется доступ только у доверенных лиц.	Документы хранятся в режимно-секретном помещении.	Документы и правовая база не противоречит друг другу.	Документы описывают проблему с достаточной полнотой.

1.2 Свойства объекта исследования на основе морфологического анализа

Объект соответствует критериям, представленным в [2] и представляет собой информационную систему в сфере транспорта. Представленная выше таблица дает оценить базовые связи компании в техническом, социальном и правовом плане. Анализируя связи между этими тремя компетенциями, можно говорить о их безопасности внутри организации. По причине что каждая из этих связей неразрывно граничит с другими, создаются условия, в которых возможно возникновения угроз. Для их предотвращения существует множество подходов, часть из них будет описана далее.

Все сотрудники организации, которые имеют доступ к важным объектам инфраструктуры компании, работают по ключевому доступу, что позволяет контролировать местонахождение сотрудников. В организации обрабатываются, коммерческая тайна, конфиденциальные данные. Каждый из сотрудников что отвечает за работоспособность системы подписал контракт на срок в несколько лет и по истечении этого срока он не может уволиться по собственному желанию. Либо будет обложен штрафом.

Так же компания располагается во множестве собственных зданий и имеет свою территорию. Все системы связи отвечающие за безопасность здания и сотрудников (пожарная система, сигнализация), находятся в пределах охраняемой территории. Каждое из зданий имеет связь друг с другом по внутренней локальной виртуальной сети.

Организация работы в Компании Mobileye осуществляется путем взаимодействия различных отделов между собой, таких отделов как: отдел разработки, отдел коммерции, отдел продаж и прочих важных составляющих любой крупной компании. В качестве средства для коммуникаций используются автоматизированные рабочие места (АРМ), а также устройства сотовой связи. Работа внутри отдела, составление задач, уведомления для сотрудников происходит за счет использования трекинговой системы. Что позволяет следить за местонахождением сотрудников внутри здания, а также контролировать кто из него вошел и вышел. Проводится работа по установке требований для защиты объекта, обеспечивается внедрение организационных и технических мер по защите [3].

Работа каждого отдельного сотрудника как правило происходит за отдельным автоматизированным рабочим местом. На АРМ установлен антивирус, а также специализированное именно для этого сотрудника ПО, в зависимости от его рода деятельности. Все необходимые для работы программы закуплены у официальных поставщиков или их представителей, отсутствует пиратское ПО и ПО имеющее потенциальные уязвимости. Все машинные

носители информации подписаны и закреплены за каждым сотрудником, что нуждается в их доступе. Так же ведется подотчетная деятельность, направленная на сохранение текущей аппаратной конфигурации АРМов пользователей, вся периферия так же имеет свой номер, сотрудникам не допускается использовать на рабочих местах устройства связи с глобальной сетью интернет, а также ноутбуки, нетбуки и планшеты с выходом в интерент.

Так же составлены внутренние документы, описывающие базовые принципы безопасности, с которыми сотрудник должен ознакомится при приеме на работу. В них описываются базовые требования для недопущения инцидентов информационной безопасности, а также описываются последствия, если будет доказано, что по вине или по причине бездействия данного сотрудника произошла утечка коммерческой тайны, повлекшая за собой убытки, либо ослабившая позицию компании на рынке.

Каждый сотрудник обязан добросовестно выполнять поставленные перед ним задачи, и не приводить к возникновению инцидентов, направленных на деструктивное воздействие на компанию, со стороны внешних нарушителей. Нельзя приводить во внутренний контур своих знакомых или друзей, все лица, что попадают на территорию организации отмечаются в журнале на проходной, оставляют свои паспортные данные, а также высказывают цель визита. Если она покажется сотруднику проходной не объективной или же за постояльца не поручится начальник одного из отделов, то он имеет право откаать в посещении предприятия.

Такие методы защиты являются первостепенными в данной компании. Они создают базу для защищенной корпоративной среды, не позволяющей злоумышленнику легко проникнуть во внутренний сетевой контур организации. А также не дают шанса попасть внутрь организации через проходную, что в свою очередь так же повышает безопасность, обеспечиваемую для компании.

1.3 Модель угроз

Модель угроз информационной безопасности включает в себя краткое описание архитектуры изучаемого объекта, характеристику каждого из источника угроз информационной безопасности, так же модель нарушителя и актуальное описание всех угроз безопасности для защищаемого объекта.

Модель угроз безопасности информации может разрабатываться для нескольких значимых объектов, имеющих одинаковые цели создания и архитектуру, а также типовые угрозы безопасности информации.

Для определения угроз безопасности информации и разработки модели угроз безопасности информации должны применяться методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 [22].

Проектирование подсистемы безопасности значимого объекта должно осуществляться в соответствии с техническим заданием на создание значимого объекта и (или) техническим заданием (частным техническим заданием) на создание подсистемы безопасности значимого объекта с учетом модели угроз безопасности информации и категории значимости значимого объекта.

Таблица 2 - Модель угроз

Способы реализации\Особенности	Большое количество разнородных технических и программных средств	Большое количество информации различного уровня конфиденциальности	Компоненты многих ИС разнесены территориально	В составе ИС присутствуют подсистемы с различными требованиями по уровням	Расширенная форма обратной связи между главным и офисами	Передача данных между офисами используются системы связи от различных производителей с разными характеристиками и

				защищенности		годами выпуска
1	Использование недекларированных возможностей операционных систем	Доступ без авторизации	Атака типа "человек посередине" путем создания поддельной точки доступа	Нарушение изоляции процессов	Использование недостатков, связанных с отсутствием проверки достоверности отправителя и/или получателя	Эксплуатация недостатков, децентрализованного и неконтролируемого подключения к сети Интернет
2	Модификация ОС (подмена системных файлов, внедрение вредоносного кода в системные процессы и ядро	Повреждение загрузочной области	Атаки на уровне каналов и сети, приводящие к изменению маршрутов	Нарушение сетевой изоляции	Атаки через социальные сети	Использование недостатков конфигурации
3	Внедрение закладок, имитирую	Затирание данных (wiping)	Врезка в линию связи	Выход за пределы замкнут	Веб-фишинг	Перенаправление трафика

	щих интерфейсы служебных программ		считывающего устройства не вразрыв (физическое подключение к проводам)	ой программной среды		
4	Внедрение закладок в системы Out-of-Band управления (Intel ME, iDrac, iLo etc)	Искажение данных	Зеркалирование трафика	Выход за пределы виртуальной инфраструктуры	Почтовый фишинг	Зеркалирование трафика

1.3.1 Описание способов реализации и угроз

1.Использование недикларированных возможностей операционных систем.

Уровень возможностей нарушителя по классификации ФСТЭК – В.4 Обладают всеми возможностями нарушителей со средними возможностями. Имеет возможность получения доступа к исходному коду встраиваемого программного обеспечения аппаратных платформ, системного и прикладного программного обеспечения, телекоммуникационного оборудования и других программно-аппаратных средств для получения сведений об уязвимостях «нулевого дня». Имеет возможность внедрения программных (программно-аппаратных) закладок или уязвимостей на различных этапах поставки программного обеспечения или программно-аппаратных средств. Имеет

возможность создания методов и средств реализации угроз с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение. Имеет возможность реализовывать угрозы с привлечением специалистов, имеющих базовые повышенные, средние и высокие возможности. Имеет возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений. Имеет возможность долговременно и незаметно для операторов систем и сетей реализовывать угрозы безопасности информации. Обладает исключительными знаниями и практическими навыками о функционировании систем и сетей, операционных систем, аппаратном обеспечении, а также осведомлены о конкретных защитных механизмах, применяемых в программном обеспечении, программно-аппаратных средствах атакуемых систем и сетей. Таким образом, нарушители с высокими возможностями имеют практически неограниченные возможности реализовывать угрозы, в том числе с использованием недекларированных возможностей, программных, программно-аппаратных закладок, встроенных в компоненты систем и сетей [18].

УБИ.1 Угроза утечки

УБИ.2 Угроза несанкционированного

УБИ.3 Угроза несанкционированной модификации (искажения)

УБИ.4 Угроза несанкционированной

УБИ.5 Угроза удаления информационных ресурсов

УБИ.6 Угроза отказа в обслуживании

2. Модификация операционной системы путем загрузки с внешнего носителя

Уровень возможностей нарушителя по классификации ФСТЭК – В.2

Обладает всеми возможностями нарушителей с базовыми возможностями. Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети Интернет и разработанные другими лицами,

однако хорошо владеют этими средствами и инструментами, понимают, как они работают и могут вносить изменения в их функционирование для повышения эффективности реализации угроз. Оснащен и владеет фреймворками и наборами средств, инструментов для реализации угроз безопасности информации и использования уязвимостей. Имеет навыки самостоятельного планирования и реализации сценариев угроз безопасности информации [18]. Обладает практическими знаниями о функционировании систем и сетей, операционных систем, а также имеют знания защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах. Таким образом, нарушители с базовыми повышенными возможностями имеют возможность реализовывать угрозы, в том числе направленные на неизвестные (недокументированные) уязвимости, с использованием специально созданных для этого инструментов, свободно распространяемых в сети «Интернет». Не имеют возможностей реализации угроз на физически изолированные сегменты систем и сетей.

Обладает следующими угрозами, описанными выше:

УБИ.2 Угроза несанкционированного доступа

УБИ.3 Угроза несанкционированной модификации (искажения)

УБИ.4 Угроза несанкционированной подмены

УБИ.5 Угроза удаления информационных ресурсов

УБИ.6 Угроза отказа в обслуживании

УБИ.7 Угроза ненадлежащего (нецелевого) использования

УБИ.8 Угроза нарушения функционирования (работоспособности)

3. Внедрение закладок, имитирующих интерфейсы служебных программ

Уровень возможностей нарушителя по классификации ФСТЭК – В.3

Обладает всеми возможностями нарушителей с базовыми повышенными возможностями. Имеет возможность приобретать информацию об уязвимостях, размещаемую на специализированных платных ресурсах (биржах уязвимостей). Имеет возможность приобретать дорогостоящие средства и инструменты для

реализации угроз, размещаемую на специализированных платных ресурсах (биржах уязвимостей). Имеет возможность самостоятельно разрабатывать средства (инструменты), необходимые для реализации угроз (атак), реализовывать угрозы с использованием данных средств [18]. Имеет возможность получения доступа к встраиваемому программному обеспечению аппаратных платформ, системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-аппаратным средствам для проведения их анализа. Обладает знаниями и практическими навыками проведения анализа программного кода для получения информации об уязвимостях. Обладает высокими знаниями и практическими навыками о функционировании систем и сетей, операционных систем, а также имеют глубокое понимание защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах. Имеет возможность реализовывать угрозы безопасности информации в составе группы лиц. Таким образом, нарушители со средними возможностями имеют возможность реализовывать угрозы, в том числе на выявленные ими неизвестные уязвимости, с использованием самостоятельно разработанных для этого инструментов. Не имеют возможностей реализации угроз на физически изолированные сегменты систем и сетей [18].

УБИ.1 Угроза утечки

УБИ.2 Угроза несанкционированного доступа

УБИ.3 Угроза несанкционированной модификации (искажения)

УБИ.4 Угроза несанкционированной подмены

УБИ.5 Угроза удаления информационных ресурсов

УБИ.6 Угроза отказа в обслуживании

УБИ.7 Угроза ненадлежащего (нецелевого) использования

УБИ.8 Угроза нарушения функционирования (работоспособности)

УБИ.9 Угроза получения информационных ресурсов из недоверенного или скомпрометированного источника

УБИ.10 Угроза распространения противоправной

УБИ.11 Угроза несанкционированного массового сбора Внедрение закладок в системы Out-of-Band управления (Intel ME, iDrac, iLo etc)

Уровень возможностей нарушителя по классификации ФСТЭК – В.3

УБИ.1 Угроза утечки

УБИ.2 Угроза несанкционированного доступа

УБИ.3 Угроза несанкционированной модификации (искажения)

УБИ.4 Угроза несанкционированной подмены

УБИ.5 Угроза удаления информационных ресурсов

УБИ.6 Угроза отказа в обслуживании

УБИ.7 Угроза ненадлежащего (нецелевого) использования

УБИ.8 Угроза нарушения функционирования (работоспособности)

УБИ.9 Угроза получения информационных ресурсов из недоверенного или скомпрометированного источника

УБИ.10 Угроза распространения противоправной информации

УБИ.11 Угроза несанкционированного массового сбора информации

4. Доступ без авторизации

Уровень возможностей нарушителя по классификации ФСТЭК – В.1

Имеет возможность при реализации угроз безопасности информации использовать только известные уязвимости, скрипты и инструменты. Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети Интернет и разработанные другими лицами, имеют минимальные знания механизмов их функционирования, доставки и выполнения вредоносного программного обеспечения, эксплойтов. Обладает базовыми компьютерными знаниями и навыками на уровне пользователя. Имеет возможность реализации угроз за счет физических воздействий на технические средства обработки и хранения информации, линий связи и обеспечивающие системы систем и сетей при наличии физического доступа к ним. Таким образом, нарушители с базовыми возможностями имеют возможность реализовывать

только известные угрозы, направленные на известные (документированные) уязвимости, с использованием общедоступных инструментов [18].

УБИ.1 Угроза утечки

УБИ.2 Угроза несанкционированного доступа

УБИ.3 Угроза несанкционированной модификации (искажения)

УБИ.4 Угроза несанкционированной подмены

УБИ.5 Угроза удаления информационных ресурсов

УБИ.6 Угроза отказа в обслуживании

УБИ.7 Угроза ненадлежащего (нецелевого) использования

УБИ.8 Угроза нарушения функционирования (работоспособности)

УБИ.9 Угроза получения информационных ресурсов из недоверенного или скомпрометированного источника

УБИ.10 Угроза распространения противоправной информации

УБИ.11 Угроза несанкционированного массового сбора информации

5. Повреждение загрузочной области

Уровень возможностей нарушителя по классификации ФСТЭК – В.2

УБИ.3 Угроза несанкционированной модификации (искажения)

УБИ.8 Угроза нарушения функционирования (работоспособности)

6. Затирание данных (wiping)

Уровень возможностей нарушителя по классификации ФСТЭК – В.2

УБИ.3 Угроза несанкционированной модификации (искажения)

УБИ.5 Угроза удаления информационных ресурсов

УБИ.6 Угроза отказа в обслуживании

УБИ.8 Угроза нарушения функционирования (работоспособности)

7. Искажение данных

Уровень возможностей нарушителя по классификации ФСТЭК – В.2

УБИ.3 Угроза несанкционированной модификации (искажения)

УБИ.5 Угроза удаления информационных ресурсов

УБИ.6 Угроза отказа в обслуживании

УБИ.8 Угроза нарушения функционирования (работоспособности)

8. Атака типа "человек посередине" путем создания поддельной точки доступа

Уровень возможностей нарушителя по классификации ФСТЭК – В.1

УБИ.1 Угроза утечки

УБИ.2 Угроза несанкционированного доступа

УБИ.3 Угроза несанкционированной модификации (искажения)

УБИ.4 Угроза несанкционированной подмены

УБИ.5 Угроза удаления информационных ресурсов

9. Атаки на уровне каналов и сети, приводящие к изменению маршрутов

Уровень возможностей нарушителя по классификации ФСТЭК – В.2

УБИ.1 Угроза утечки

УБИ.2 Угроза несанкционированного доступа

УБИ.3 Угроза несанкционированной модификации (искажения)

УБИ.4 Угроза несанкционированной подмены

УБИ.5 Угроза удаления информационных ресурсов

10. Врезка в линию связи считывающего устройства не вразрыв (физическое подключение к проводам)

Уровень возможностей нарушителя по классификации ФСТЭК – В.2

УБИ.1 Угроза утечки

УБИ.2 Угроза несанкционированного доступа

УБИ.11 Угроза несанкционированного массового сбора информации

11. Зеркалирование трафика

Уровень возможностей нарушителя по классификации ФСТЭК – В.1

УБИ.1 Угроза утечки

УБИ.2 Угроза несанкционированного доступа

УБИ.11 Угроза несанкционированного массового сбора информации

12. Нарушение изоляции процессов

Уровень возможностей нарушителя по классификации ФСТЭК – В.3

УБИ.1 Угроза утечки

УБИ.2 Угроза несанкционированного доступа

УБИ.3 Угроза несанкционированной модификации (искажения)

УБИ.4 Угроза несанкционированной подмены

УБИ.5 Угроза удаления информационных ресурсов

УБИ.8 Угроза нарушения функционирования (работоспособности)

УБИ.10 Угроза распространения противоправной информации

13. Выход за пределы замкнутой программной среды

Уровень возможностей нарушителя по классификации ФСТЭК – В.3

УБИ.1 Угроза утечки

УБИ.2 Угроза несанкционированного доступа

УБИ.3 Угроза несанкционированной модификации (искажения)

УБИ.4 Угроза несанкционированной подмены

УБИ.5 Угроза удаления информационных ресурсов

УБИ.8 Угроза нарушения функционирования (работоспособности)

УБИ.10 Угроза распространения противоправной информации

14. Выход за пределы виртуальной инфраструктуры

Уровень возможностей нарушителя по классификации ФСТЭК – В.3

УБИ.1 Угроза утечки

УБИ.2 Угроза несанкционированного доступа

УБИ.3 Угроза несанкционированной модификации (искажения)

УБИ.4 Угроза несанкционированной подмены

УБИ.5 Угроза удаления информационных ресурсов

УБИ.8 Угроза нарушения функционирования (работоспособности)

УБИ.10 Угроза распространения противоправной информации

15. Нарушение сетевой изоляции

Уровень возможностей нарушителя по классификации ФСТЭК – В.3

УБИ.1 Угроза утечки

УБИ.2 Угроза несанкционированного доступа

УБИ.3 Угроза несанкционированной модификации (искажения)

УБИ.4 Угроза несанкционированной подмены

УБИ.5 Угроза удаления информационных ресурсов

УБИ.8 Угроза нарушения функционирования (работоспособности)

УБИ.10 Угроза распространения противоправной информации

16. Использование недостатков, связанных с отсутствием проверки достоверности отправителя и/или получателя

Уровень возможностей нарушителя по классификации ФСТЭК – В.3

УБИ.1 Угроза утечки

УБИ.2 Угроза несанкционированного доступа

УБИ.3 Угроза несанкционированной модификации (искажения)

УБИ.4 Угроза несанкционированной подмены

УБИ.5 Угроза удаления информационных ресурсов

УБИ.6 Угроза отказа в обслуживании

УБИ.7 Угроза ненадлежащего (нецелевого) использования

УБИ.8 Угроза нарушения функционирования (работоспособности)

УБИ.9 Угроза получения информационных ресурсов из недоверенного или скомпрометированного источника

УБИ.10 Угроза распространения противоправной информации

УБИ.11 Угроза несанкционированного массового сбора информации

17. Атаки через социальные сети

Уровень возможностей нарушителя по классификации ФСТЭК – В.1

УБИ.1 Угроза утечки

УБИ.2 Угроза несанкционированного доступа

УБИ.3 Угроза несанкционированной модификации (искажения)

УБИ.5 Угроза удаления информационных ресурсов

УБИ.8 Угроза нарушения функционирования (работоспособности)

УБИ.9 Угроза получения информационных ресурсов из недоверенного или скомпрометированного источника

УБИ.10 Угроза распространения противоправной информации

УБИ.11 Угроза несанкционированного массового сбора информации

18. Веб-фишинг

Уровень возможностей нарушителя по классификации ФСТЭК – В.1

УБИ.1 Угроза утечки

УБИ.2 Угроза несанкционированного доступа

УБИ.3 Угроза несанкционированной модификации (искажения)

УБИ.5 Угроза удаления информационных ресурсов

УБИ.8 Угроза нарушения функционирования (работоспособности)

УБИ.9 Угроза получения информационных ресурсов из недоверенного или скомпрометированного источника

УБИ.10 Угроза распространения противоправной информации

УБИ.11 Угроза несанкционированного массового сбора информации

19. Почтовый фишинг

Уровень возможностей нарушителя по классификации ФСТЭК – В.1

УБИ.1 Угроза утечки

УБИ.2 Угроза несанкционированного доступа

УБИ.3 Угроза несанкционированной модификации (искажения)

УБИ.5 Угроза удаления информационных ресурсов

УБИ.8 Угроза нарушения функционирования (работоспособности)

УБИ.9 Угроза получения информационных ресурсов из недоверенного или скомпрометированного источника

УБИ.10 Угроза распространения противоправной информации

УБИ.11 Угроза несанкционированного массового сбора информации

20. Эксплуатация недостатков, децентрализованного и неконтролируемого подключения к сети Интернет

Уровень возможностей нарушителя по классификации ФСТЭК – В.1

УБИ.1 Угроза утечки

УБИ.2 Угроза несанкционированного доступа

УБИ.3 Угроза несанкционированной модификации (искажения)

УБИ.4 Угроза несанкционированной подмены

УБИ.5 Угроза удаления информационных ресурсов

УБИ.6 Угроза отказа в обслуживании

УБИ.7 Угроза ненадлежащего (нецелевого) использования

УБИ.9 Угроза получения информационных ресурсов из недоверенного или скомпрометированного источника

УБИ.10 Угроза распространения противоправной информации

УБИ.11 Угроза несанкционированного массового сбора информации

21. Использование недостатков конфигурации

Уровень возможностей нарушителя по классификации ФСТЭК – В.2

УБИ.1 Угроза утечки

УБИ.2 Угроза несанкционированного доступа

УБИ.3 Угроза несанкционированной модификации (искажения)

УБИ.4 Угроза несанкционированной подмены

УБИ.5 Угроза удаления информационных ресурсов

УБИ.6 Угроза отказа в обслуживании

УБИ.7 Угроза ненадлежащего (нецелевого) использования

УБИ.8 Угроза нарушения функционирования (работоспособности)

УБИ.9 Угроза получения информационных ресурсов из недоверенного или скомпрометированного источника

УБИ.10 Угроза распространения противоправной информации

УБИ.11 Угроза несанкционированного массового сбора информации

22. Перенаправление трафика

Уровень возможностей нарушителя по классификации ФСТЭК – В.3

УБИ.1 Угроза утечки

УБИ.2 Угроза несанкционированного доступа

УБИ.6 Угроза отказа в обслуживании

УБИ.8 Угроза нарушения функционирования (работоспособности)

УБИ.11 Угроза несанкционированного массового сбора информации

23. Зеркалирование трафика

Уровень возможностей нарушителя по классификации ФСТЭК – В.1

УБИ.1 Угроза утечки

УБИ.2 Угроза несанкционированного доступа

УБИ.11 Угроза несанкционированного массового сбора информации

1.3.2 Модель нарушителя

Методом экспертной оценки были выявлены 2 потенциальных вида нарушителей, внешний и внутренний.

Среди внутренних нарушителей в первую очередь можно выделить:

- Обнаружение непосредственных пользователей операционной системы, включая руководителей разного уровня;
- Администраторы компьютерных сетей и информационной безопасности;
- Программисты приложений и систем;
- Персонал службы безопасности;
- Специалисты по обслуживанию зданий и компьютеров, от уборщиков до сервисных инженеров;
- Вспомогательный персонал и временные работники.

Среди основных причин, которые могут побудить сотрудников к неправомерным действиям можно:

- безответственность;
- ошибки пользователя и администратора;
- Демонстрация собственного превосходства (самоутверждение);
- «борьба с системой»;
- частные интересы пользователей системы;
- Использование несовершенства системы информационных технологий.

Группы внешних нарушителей может представлять:

- клиент;
- приглашенные посетители;
- представители объединенной организации;

- Работники отраслевых регулирующих органов;
- нарушение правил доступа к объекту;
- Наблюдатели за охраняемой территорией.

Кроме того, есть возможность классифицировать по заданным параметрам.

Используемые методы и средства:

- Сбор информации и данных;
- Пассивные средства перехвата;
- Использование средств, содержащихся в информационной системе или ее защите, и недостатки;

Осведомленность правонарушителя о корпоративной структуре:

- Типичные знания методов построения компьютерных систем, сетевых протоколов с использованием стандартных сборок;
- Высокий уровень технических знаний, опыт работы со специализированными программными продуктами и утилитами;
- Обширные знания в области программирования, системного проектирования и эксплуатации компьютерных систем;
- Получить информацию о носителе и механизмах защиты атакуемой системы;
- Нарушители — разработчики или участники системы безопасности.

Время информационного воздействия:

- При обработке информации;
- Во время передачи данных;
- При хранении данных (с учетом постоянного и нерабочего состояния системы).

Метод реализации в зависимости от воздействия:

- Дистанционное использование для перехвата информации, передаваемой по каналам передачи данных, либо ее неиспользование;
- доступ к охраняемым территориям;

- Непосредственный физический контакт с вычислительным оборудованием, при этом различая: доступ к рабочим станциям, доступ к корпоративным серверам, доступ к системам управления, контроля и управления информационными системами, доступ к программам управления системами информационной безопасности

Рассмотрены типовые угрозы и составлена модель нарушителя [4].

1.3.3 Особенности КИИ

Изучив историю развития компании Mobileye, а также ее продвижение по рынку, можно сказать что на данный момент информационная структура компании представляет собой достаточно объемную информационную систему, которая в части своей деятельности связанна с обеспечением безопасности населения на дорогах, а также описанных выше критериях. Что дает право судить о ее принадлежности к критической информационной инфраструктуре, в соответствии с [2].

Как и любая другая КИИ, эта не лишена своих особенностей, выделенных в ходе экспертной оценки, в частности:

1. В эксплуатации находится большое количество разнородных технических и программных средств
2. В базах данных содержится большое количество информации различного уровня конфиденциальности
3. Компоненты многих ИС разнесены территориально
4. В составе ИС присутствуют подсистемы с различными требованиями по уровням защищенности
5. Для передачи данных между офисами используются системы связи от различных производителей с разными характеристиками и годами выпуска.

Выделив особенности КИИ на примере компании Mobileye, можно составить матрицу угроз, соотносящимися с этими особенностями.

Разбор особенностей рабочего процесса, описание свойств КИИ [19].

1.3.4 Обзор существующей методики по определению угроз безопасности информации

В данном параграфе будет рассмотрен документ «Методический документ. Методика оценки угроз безопасности информации от 5 февраля 2021г». Как и многие, этот является одним из наиболее важных при построении устойчивой распределенной информационной системы.

На сегодняшний день оценка возможности реализации угроз безопасности информации складывается из нескольких пунктов [21]:

1. Предлагается изучить общий перечень угроз безопасности информации, который представлен на сайте ФСТЭК.
2. Описать векторы компьютерных атак, содержащиеся в других источниках, например: CAPEC, ATT&CK, OWASP, STIX, WASC.
3. Изучить документацию по используемым сетям и системам. Знать типы архитектур, групп пользователей и использованные внутренние и внешние выходы сети.
4. Оценить возможный ущерб при реализации атаки.
5. Определить объекты воздействий угроз безопасности информации.
6. Выявить виды и категории антропогенных нарушителей, которые смогут реализовать атаку, даже непреднамеренную.

Обращаясь к [21], в пункте 5.2.2 мы видим рекомендации, нацеленные на определение типовых угроз, но нигде не сказано, как эту вероятность высчитывать.

Как вариант решения данной проблемы, предлагаю рассмотреть свой подход, основанный на экспертной оценке. Он заключается в рассмотрении типовых угроз, анализе наиболее вероятного вектора атак по Miter Mattrix, моделирование распределенной информационной системы, сбора статистики от экспертов в сфере информационной безопасности, а также расчета вероятности

возникновения того или иного события информационной безопасности. Такой подход может многократно повысить достоверность оцениваемой экспертом системы, что позволит быстрее вводить инженерные решения в области информационной безопасности в систему, сделает акцент на вероятных угрозах более узким, что даст возможность концентрировать средства защиты на конкретных уязвимостях.

1.3.5 Численный расчет безопасности защищаемой системы.

Формальная модель оценки защищенности системы на примере компании Mobileye. Сформированная модель позволит составить достоверный стенд, исходя из ее описания. Так же эта модель послужит вводными данными в проводимом исследовании.

Данные расчеты помогут однозначно вычислить достоверность оцениваемой экспертом системы. Так как высчитав численные значения мы сможем получить результат, опираясь на который можно будет сформулировать итоги поставленной задачи.

За основу расчетной базы было взято определение доверительного интервала. Этот статистический метод оценки может показать такой интервал изменения случайной величины, который с заданной вероятностью, накроет истинное значение оцениваемого параметра распределения и не будет брать в расчет значения, выходящие за его пределы. Это позволит оценить вероятности того или иного события с большей точностью, что скажется на качестве проводимого исследования.

Для реализации расчета данным методом необходимо собрать оценки экспертов по информационной безопасности. Для репрезентативности данной выборки будут участвовать специалисты из разных возрастных групп, с разным опытом работы.

Выполнение расчета доверительного интервала состоит из обработки собранных статистических данных [20].

Первым что необходимо будет получить – это Среднее арифметическое между всеми значениями генеральной выборки. Оно рассчитывается по формуле:

$$\bar{x} = \frac{\sum x}{n} (1)$$

Где:

- $\bar{x}$, является оценкой среднего генеральной совокупности данных что мы имеем

- n, количество данных, которые мы получили

- x, значения, которые нам необходимо просуммировать

Следующим этапом нужно будет посчитать среднеквадратичное отклонение от нашей выборки. Это значение поможет оценить степень рассеивания всех значений что мы получили, то есть насколько сильно один запрос отличается от другого исходя из выбранного множества. Она рассчитывается по формуле:

$$\sigma = \sqrt{\frac{\sum(x-\bar{x})^2}{n}} (2)$$

Затем нужно выбрать значение доверительного интервала. Наиболее часто используемый доверительный уровень 95%.

После этого мы рассчитываем предел погрешности. Он рассчитывается из произведения доверительного отношения на стандартную ошибку:

$$Z_{\frac{\alpha}{2}} \frac{\sigma}{\sqrt{n}} (3)$$

В конце мы сможем найти границы доверительного интервала, которые покажут нам диапазон, в котором находится истинный ответ среди всей генеральной выборки, с заданной точностью. Он считается по формуле по этой формуле:

$$\bar{x} \pm Z_{\frac{\alpha}{2}} \frac{\sigma}{\sqrt{n}} (4)$$

Вывод по первой главе:

В данной главе был проведен анализ объекта – корпорация Mobileye, с целью определить является ли данный субъект, объектом критической информационной инфраструктуры, для дальнейшего обеспечения его безопасности в рамках требования [1].

Были рассмотрены процессы, обеспечивающие функционирование субъекта. На основаниях приведенного перечня процессов был сформирован список возможных угроз и описаны основные методы их реализации в соответствии с описанием БДУ ФСТЭК.

Выделенная компания относится к объекту в сфере транспорта, что позволяет отнести ее к критической информационной инфраструктуре, а сам субъект назвать субъектом КИИ.

Следующим этапом в реализации цели дипломной работы будет служить: выделение общих уязвимостей в различных компаниях, определение наиболее актуального вектора атаки, моделирование работы отдела компании Mobileye, а также, расчет ширины доверительного интервала на примере стенда с последующим анализом результата.

ГЛАВА 2. ИССЛЕДОВАНИЕ ВОПРОСА ОПРЕДЕЛЕНИЯ ТИПОВЫХ КОМПЬЮТЕРНЫХ АТАК НА РАЗНЫЕ ВИДЫ ОРГАНИЗАЦИЙ И РЕАГИРОВАНИЯ РАСПРЕДЕЛЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ НА НИХ.

2.1 Определения наиболее вероятных компьютерных угроз для организаций, относящихся к КИИ

С учетом быстрорастущего темпа цифровизации организаций, возрастает плацдарм для новых компьютерных угроз. Эта тенденция делает работу специалиста по информационной безопасности все более актуальной. Также это свидетельствует о том, что для решения вопроса безопасности организации нужно обращать внимание на наиболее вероятные компьютерные атаки, так как зачастую они носят массовый характер и имеют отношение к любой компании, не зависимо от ее рода деятельности [14]. Далее будут рассмотрены различные типы организации для выявления наиболее вероятной угрозы, которая может возникнуть в компании.

2.1.1 Основные типы компьютерных атак в сфере кредитно-финансовых организаций

В этой главе представлена информация об основных типах атак в финансовом секторе, которые FinCERT задокументирует в 2021 и 2022 годах. Если в 2021 году Банк России наблюдал непрерывную смену угроз кредитно-финансовому сектору, то в 2022 году характер угроз будет определяться эпидемией новой коронавирусных инфекций. Неожиданно она фактически стала «черным лебедем», кардинально и негативно изменившим все стороны общественной и экономической жизни, в том числе обеспечение информационной безопасности финансовых организаций и их клиентов. Основная роль заключается в переводе коммерческой, социальной и бытовой хозяйственной деятельности в дистанционный формат.

Атаки на клиентов банков (держателей карт и счетов) с использованием методов социальной инженерии продемонстрировали значительный рост объемов и прогресс в плане воздействия. Добавление личных данных, полученных из различных источников, к вводящей в заблуждение схеме, а также использование более узких, индивидуальных методов социальной инженерии в течение периода проверки значительно повысили эффективность и прибыльность того, что казалось хорошо зарекомендовавшим себя так называемым телефонным преступлением, мошенничества в компании.

Спрос на конфиденциальные данные клиентов, используемые для дальнейших различных махинаций, привел к резкому росту рынка услуг, позволяющих осуществлять незаконный доступ к базам данных финансовых учреждений и «взламывать» счета клиентов. Весь рассматриваемый период отмечен резонансными утечками из финансовых и иных организаций, не подконтрольных Банку России.

Еще одной важной тенденцией этого года является то, что количество наиболее опасных целевых атак на информационную инфраструктуру финансовых организаций продолжило многолетнее снижение практически до полной остановки. Массовая рассылка списков адресов сотрудников вредоносными программами, такими как Cobalt Strike и Silence, которые в последние несколько лет привлекали особое внимание индустрии информационной безопасности, практически прекратилась [5]. По сравнению с предыдущими годами несколько успешных взломов привели к минимальному ущербу. Кроме того, практически полностью прекратились атаки на банковские устройства самообслуживания. В то же время, исходя из данных Банка России, можно предположить, что как минимум одна группа злоумышленников ориентирована на квалифицированный взлом финансовых мобильных приложений.

Выделяя основные тезисы из вышенаписанного можно сделать следующий вывод. Для сферы банкинга основными видами угроз являются:

1. Социальная инженерия, нацеленная на атаки в сторону потребителей
2. Превышение полномочий со стороны внутренних сотрудников
3. Использование специализированных программ, нацеленных на атаки банковских систем. (Cobalt Strike, Silence)
4. Использование вирусов шифровальщиков

2.1.2 Основные типы компьютерных атак на промышленные предприятия

С точки зрения информационной безопасности компоненты системы автоматизации управления современными промышленными предприятиями являются наиболее важными, но и слабозащищенными объектами. Успешные атаки на них опасны прежде всего не экономическими потерями, а чрезвычайными ситуациями, которые могут привести к временным отключениям или нарушениям движения транспорта и связи, а также к крупным техногенным катастрофам и человеческим жертвам.

Слабые места безопасности в компонентах АСУ ТП являются результатом множества факторов, в большинстве случаев схожих с проблемами в типичных корпоративных сетях. Однако природа систем автоматического управления накладывает определенные ограничения на механизмы безопасности.

В большинстве промышленных компаний можно выйти за границы сети и получить доступ к сегментам корпоративной локальной сети. Большинство нарушений безопасности на сетевом периметре связано с ошибками конфигурации. В то же время многие промышленные организации не готовы противостоять внутренним злоумышленникам, пытающимся проникнуть в их контур [17].

В каждой промышленной организации, в которой удалось получить доступ к ИС из вне, был обнаружен какой-либо недостаток в сегментации сети или фильтрации трафика. При этом в 64 процентах компаний эти недостатки были внесены администраторами при создании каналов удаленного

управления, а в 18 процентах компаний ресурсы АСУ вообще не выделялись в отдельные сетевые сегменты.

Среди всех выявленных векторов атак, направленных на вывод ИС из строя, они характеризовались низкой или незначительной сложностью. Для их реализации достаточно использовать существующие недостатки в конфигурации устройств и сегментации сети, а также уязвимости операционной системы, которые можно найти в Интернете.

Словарные пароли и устаревшие версии программ с известными уязвимостями были обнаружены в РИС почти каждой промышленной компании. Именно эти недостатки позволяют развивать векторы атак для получения максимальных привилегий в домене и контроля над всей корпоративной инфраструктурой.

Наличие интерфейса управления РИС и удаленного доступа к СУБД сторонними злоумышленниками, наряду с широким использованием словарей и стандартных паролей для привилегированных пользователей, позволяет в один шаг получить полный контроль над веб-приложениями и серверами, получить доступ к базам данных и файлам, для запуска атаки на другие ресурсы. Важные данные, хранящиеся в открытом доступе, такие как учетные записи, исходный код веб-приложений, личные данные пользователей, могут быть использованы в атаках [17].

Такие уязвимости, как «удаленное выполнение команд» и «произвольная загрузка файлов», могут быть использованы за пределами промышленных компаний, если веб-приложение находится на сервере, подключенном к внешней сети.

Поскольку веб-приложения не являются частью промышленной организации РИС, их безопасности уделяется мало внимания. Согласно исследованию, почти каждое второе веб-приложение (43%) имеет крайне низкий уровень безопасности на периметре промышленных компаний.

Устаревшие версии программного обеспечения (например, веб-серверы, операционные системы, системы приложений) часто содержат критические уязвимости, которые злоумышленники могут использовать для получения контроля над ресурсами. Многие из этих уязвимостей имеют общедоступные эксплойты. Неправильные настройки не менее опасны: чрезмерные привилегии СУБД или веб-сервера позволяют (при доступе к ним) выполнять команды операционной системы на сервере с максимальными привилегиями. Даже ограниченные привилегии в серверных операционных системах, расположенных на сетевом периметре, но также имеющих веб-интерфейс, позволяют злоумышленникам разрабатывать векторы атак, направленные на внутренние ресурсы компании.

Рассмотрев приведенные недостатки РИС предприятия можно выделить следующие векторы атак:

1. Недостатки безопасности при построении ЛВС
2. Использование устаревших версий ОС и ПО
3. Использование простых паролей
4. Хранение в открытом доступе информации о сотрудниках
5. При наличии веб сервисов, небезопасное написание программного кода приложений
6. Неосторожность пользователя

2.1.3 Основные типы компьютерных атак на частные организации

Типовые угрозы для частных компаний:

В условиях стремительного роста предпринимательской активности сохранение лидирующих позиций на рынке является одной из важнейших задач. Это невозможно без обеспечения безопасности бизнеса и его сотрудников. Раскрытие природы безопасности тесно связано с понятием угроз безопасности от различных источников опасности. Источники опасности

скрыты и при определенных условиях обнаруживаются враждебные намерения, вредные свойства, деструктивные условия и факторы.

Многие компании не хотят покупать лицензии на профессиональное ПО из соображений экономии, поэтому стараются найти бесплатные аналоги этих программ. К сожалению, такая экономия может иметь плачевные последствия, так как пиратские копии часто содержат вредоносный код (вирусы) и незадекларированный функционал, позволяющий злоумышленникам незаметно похитить информацию.

Поскольку сотрудники самостоятельно отключают средства защиты, система безопасности данных находится под угрозой [13]. Это сделано для упрощения работы, чтобы было проще входить в систему и выполнять должностные обязанности без необходимости вводить пароли и ждать проверки.

Необходимо предоставлять доступ к определенным частям системы только тем сотрудникам, которые непосредственно работают с этими частями и соответствующими функциями.

Многие руководители компаний часто забывают, что конфиденциальной информацией нельзя делиться с друзьями и семьей, не говоря уже о незнакомцах и конкурентах.

Администратор безопасности должен убедиться, что антивирусное программное обеспечение и его сигнатуры всегда обновлены. И лучше всего настраивать обновления таким образом, чтобы они происходили централизованно и без участия пользователя, что исключает человеческий фактор.

Утеря карт флэш-памяти, дисков или даже целых ноутбуков — еще одна причина утечки конфиденциальных данных. Кроме того, кража таких носителей часто становится целью злоумышленников и конкурентов. Пользователи должны быть проинструктированы о правилах обращения с носителями конфиденциальной информации. Использование внешних

носителей информации по причинам, неизвестным ответственным лицам, должно быть запрещено внутри организации. Та же DLP-система [12] может использоваться для ограничения подключений к внешним носителям и загрузки на них конфиденциальной информации.

Во многих компаниях сотрудники не понимают основных принципов информационной безопасности. Необходимо разъяснить сотрудникам важность блокировки компьютеров при уходе с рабочего места в случае необходимости. К сожалению, многие люди забывают об этом, что также влечет за собой определенный риск утечки данных. В конце концов, сотрудники не контролируют свои компьютеры, если они не находятся на рабочем месте.

1. Использование пиратского ПО
2. Низкая осведомленность сотрудников о ИБ
3. Отсутствие разграничения доступа
4. Разглашение конфиденциальной информации
5. Редкое обновление антивирусных баз
6. Потеря носителей конфиденциальной информации
7. Отсутствие блокировки компьютера на время отсутствия пользователя
8. Неосведомленность пользователей о базовых принципах информационной безопасности

Подводя итоги по определению наиболее вероятных компьютерных атак для организаций, являющихся КИИ можно сказать следующее. Как видно из описания все они имеют свои особенности, но также не лишены сходств. Первое и самое очевидное – это люди, точнее человеческий фактор. Почти любой из сотрудников этих сфер, который имеет на своем рабочем месте доступ в интернет и возможность просматривать корпоративный почтовый ящик, может стать потенциальной жертвой в планах киберпреступника. Невнимательность или неосведомленность сотрудника, открывшего почтовый ящик компании может стоить ей репутации, а также колоссального количества денег, времени и

репутации. Все потому, что под видом обычного вложенного документа в почтовое сообщение от, казалось, бы постоянного партнера по бизнесу или регулятора, может скрываться один из множества вшитых в файл вирусов. Наиболее вероятные угрозы, которые может понести такой файл – это вшитый в него вирус «Шифровальщик - вымогатель» или «Сетевой червь». Описание работы этих угроз, а также последствия их попадания на компьютер пользователя будут рассмотрены далее.

2.2 Определение наиболее распространенных компьютерных атак.

В настоящее время в Интернете имеется множество ресурсов, с помощью которых злоумышленники могут проникнуть в компьютерные сети. Подробности об уязвимостях программного обеспечения публично обсуждаются в группах новостей и на профессиональных ресурсах [11]. Существуют готовые руководства по атакам, описывающие, как писать программы для проникновения в компьютерные сети, используя информацию об уязвимостях программ. Написаны тысячи таких программных инструментов, которые позволяют любому предотвратить компьютерные атаки. Описания компьютерных атак больше не появлялись на пиратских BBS, известных лишь небольшому кругу лиц, а публиковались на известных коммерческих сайтах [16].

Говоря о компьютерных атаках, мы в первую очередь подразумеваем получения третьими лицами несанкционированного доступа к рассматриваемой системе. Рассматривая компьютерные атаки важно учитывать их многообразие, ведь современные информационные системы сложны, что в свою очередь создает большой плацдарм для реализации атак. Наиболее частыми компьютерными атаками, выделенными исходя из метода экспертной оценки являются:

- Удаленное проникновение в компьютер: программы, которые получают неавторизованный доступ к другому компьютеру через Интернет (или локальную сеть)
- Локальное проникновение в компьютер: программы, которые получают неавторизованный доступ к компьютеру, на котором они работают.
- Удаленное блокирование компьютера: программы, которые через Интернет (или сеть) блокируют работу всего удаленного компьютера или отдельной программы на нем (для восстановления работоспособности чаще всего компьютер надо перезагрузить)
- Локальное блокирование компьютера: программы, которые блокируют работу компьютера, на котором они работают
- Сетевые сканеры: программы, которые осуществляют сбор информации о сети, чтобы определить, какие из компьютеров и программ, работающих на них, потенциально уязвимы к атакам.
- Сканеры уязвимых мест программ: программы, проверяют большие группы компьютеров в Интернете в поисках компьютеров, уязвимых к тому или иному конкретному виду атаки.
- Вскрыватели паролей: программы, которые обнаруживают легко угадываемые пароли в зашифрованных файлах паролей. Сейчас компьютеры могут угадывать пароли так быстро что, казалось бы, сложные пароли могут быть угаданы.
- Сетевые анализаторы (снифферы): программы, которые слушают сетевой трафик. Часто в них имеются возможности автоматического выделения имен пользователей, паролей и номеров кредитных карт из трафика.

2.2.1 Компьютерная атака «Сетевой червь»

Атаки «сетевых червей» остаются одной из наиболее часто используемых дыр в системе безопасности. Сетевой червь — это вредоносная программа, распространяющая свои копии в локальной или глобальной сети. Эти черви

используют службы компьютерных сетей для проникновения в устройства. Активация сетевых червей может привести к уничтожению программ и данных, а также к краже персональных данных пользователей. В классической версии сетевого червя по сети рассылаются специально созданные сетевые пакеты, в результате чего часть кода червя проникает на компьютер жертвы, инициирует загрузку основного файла вируса и запускает его для работы на зараженном компьютере.

Возьмем в качестве примера классического сетевого червя. Члены этого семейства вредоносных программ используют уязвимости в службе сервера локальной системной аутентификации (LSASS) в операционной системе (ОС) Microsoft Windows. В результате внедрения в систему червь запускает службу FTP на TCP-порту 5554, а затем запускает 128 программ-распространителей. При запуске червь пытается вызвать системную процедуру AbortSystemShutdown для предотвращения перезагрузки системы. Затем он выбирает любой IP-адрес для атаки и отправляет запрос на другой порт, чтобы проверить, работает ли служба LSASS. Если на запрос ответят, червь воспользуется уязвимостью в службе LSASS на том же порту, затем загрузит и запустит копию вредоносного кода с ранее запущенного сервера, завершив процесс проникновения и активации. [7]

После заражения инфицированная машина выводит сообщение об ошибке LSASS service failing, после чего может попытаться перезагрузиться.

Червь создает в корневом каталоге диска C: файл “win.log”, который содержит IP-адреса атакуемых машин.

Сетевому червю рассматриваемого типа присущи определенные признаки, по которым можно определить, произошло заражение компьютера программ или файлов. К таким признакам относятся:

– изменение размера файлов и даты создания;

– выдача сообщений типа «Write protect error» при чтении информации с защищенных от записи дисков;

– замедление работы программ, зависание и перезагрузка;

– уменьшение объема системной памяти и свободного места на диске без видимых причин;

– появление новых сбойных кластеров, дополнительных скрытых файлов или других изменений файловой системы;

– большое количество исходящих TCP/ IP-пакетов, расползающихся по всей сети и в большинстве адресованных несуществующим получателям;

– наличие пакетов и сообщений с подозрительным или недопустимым содержимым.

Виды наносимого вирусом ущерба:

– разрушение отдельных файлов, управляющих блоков или файловой системы в целом;

– блокирование некоторых функций ОС;

– выдача ложных, раздражающих или отвлекающих сообщений;

– создание звуковых или визуальных эффектов;

– имитация ошибок или сбоев в программе или ОС;

– имитация сбоев аппаратуры (зависание компьютера через некоторое время после включения и т. д.).

2.2.2 Компьютерная атака «Шифровальщик»

Вирусы-шифровальщики (ВШ) остаются одной из главных проблем в области защиты личных данных пользователей компьютерных систем (КС). С одной стороны, последствия заражения системы ВШ в большинстве случаев приводят к частичной или полной утере данных пользователя в силу невозможности расшифровывания этих данных [1], с другой, современные средства защиты от вредоносных программ зачастую не справляются со своей функцией и не защищают пользовательские КС от заражения. Классические методы борьбы с вредоносным программным обеспечением (ПО) остаются малоэффективными при обнаружении вредоносного кода, ранее не известного

разработчикам антивирусных программных средств и эксплуатирующего уязвимости нулевого дня.

В качестве примера рассмотрим Trojan-Downloader.MSOffice.SLoad. Одними из самых частых сетей, через которые внедряются Trojan-Downloader.MSOffice.SLoad, являются:

- С помощью фишинговых писем;
- В результате того, что клиент оказался на источнике, содержащем деструктивное программное приложение;

Как только вирус будет эффективно внедрен, он либо зашифрует данные на компьютере пользователя, либо запретит доступ на их изменение, а также поместит примечание о выкупе, в котором упоминается, что злоумышленники должны получить выплату за расшифровку данных, зашифрованных вредоносным ПО. Во многих случаях записка с требованием выкупа появляется, когда клиент перезагружает компьютер после того, как система фактически уже была повреждена.

Сам вирус представляет собой DOC/DOCX-документ, содержащий скрипт на языке VBA (Visual Basic for Applications), который может исполняться в MS Word. В скрипте содержатся процедуры для установки соединения, а также скачивания, сохранения и запуска файла. Скачанные программы, как правило, являются шифровальщиками.

Так же шифровальщик может использовать встроенные в него функции сетевого червя, что помогает ему эффективнее распространяться в локальной сети. Вирус пытается распространяться через уязвимость в SMBv1, для этого он перебирает множество IP-адресов случайным образом и пытается соединиться по порту 445 (SMB).

2.2.3 Определение вектора развития атаки в системе пользователя при помощи ATT&CK

Каждый специалист по информационной безопасности задумывался, как же защитить информационную систему пользователя или компании от постоянной угрозы со стороны хакеров, как именно та или иная уязвимость может быть проэксплуатированна, как злоумышленникам удается проникать в, казалось, бы в самые защищенные участки сети.

Чтобы ответить на эти вопросы, в 2013 году корпорация MITRE анонсировала базу знаний ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) как метод описания и классификации поведения злоумышленников на основе анализа реальных атак.

MITRE ATT&CK — это структурированный список известных действий злоумышленника, разбитый на тактики и методы и представленный в виде таблицы (матрицы). Матрица для различных ситуаций и типов злоумышленников опубликована на сайте MITRE. Эта таксономия также доступна в машиночитаемом формате STIX/TAXII. Поскольку этот список дает полное представление о том, что делают злоумышленники, когда сеть скомпрометирована, он полезен для различных мер защиты, мониторинга, обучения и других приложений.

В частности, ATT&CK полезен для кибербразведки, поскольку позволяет стандартизированным образом описать поведение злоумышленника. Злоумышленников («хакеров») можно отследить, сопоставив наблюдаемые события в сети с методами и политиками ATT&CK, использующими определенные группы. Это позволяет специалистам по информационной безопасности оценивать уровень защищенности существующих средств защиты, анализируя их способность выявлять или блокировать определенные методы и тактики, тем самым понимая сильные и слабые стороны в отношении тех или иных злоумышленников.

Хороший способ визуализировать сильные и слабые стороны охранной деятельности по отношению к конкретным группам или субъектам — это, например, создать карту технологического покрытия в Excel или с помощью навигатора MITRE ATT&CK. База знаний ATT&CK также доступна в виде источника STIX/TAXII 2.0, что позволяет легко интегрировать ее в любой инструмент, поддерживающий эту технологию.

Корпорация MITRE внесла значительный вклад в сообщество безопасности, предоставив ATT&CK, сопутствующие инструменты и ресурсы. Это сделано в удачное время. По мере того, как злоумышленники находят способы быть более незаметными и избегать обнаружения с помощью традиционных инструментов безопасности, специалисты по безопасности вынуждены менять способы обнаружения атак и защиты от них. База знаний ATT&CK изменяет наше восприятие, абстрагируя низкоуровневые индикаторы, такие как IP-адреса и доменные имена, и позволяет нам рассматривать злоумышленников и нашу защиту через призму поведения [10].

Однако это новое восприятие не означает, что работа безопасников упростится. Безоблачные дни блэклистов и простых фильтров киберразведки почти исчезли. Стратегия обнаружения и предотвращения на основе поведения злоумышленников — это гораздо более сложный путь, чем инструменты прошлого, работающие по принципу «настроил и забыл». Кроме того, по мере появления новых способов защиты злоумышленники, безусловно, будут адаптироваться. ATT&CK позволяет описывать любые новые методы, которые будут использовать злоумышленники, и, будем надеяться, позволит нам не отставать.

Исходя из выше описанного, а также методики ФСТЭК, где предлагают рассмотреть данную базу знаний, можно подобрать наиболее вероятный вектор атаки, применимый к организации Mobileye.

Опираясь на данные о компании, полученные в 1 и 2 главе, а также используя метод экспертной оценки, выделим такой вектор атаки, как

«Фишинг: Прикрепление целевого фишинга», так как он имеет наиболее распространенное применение российских и зарубежных компаний.

Злоумышленники могут рассылать фишинговые электронные письма с вредоносными вложениями, пытаясь получить доступ к системе жертвы и заразить компьютер вирусом, что нарушит одно из допущений информационной безопасности — целостность. Целевая фишинговая атака — это особая разновидность целевого фишинга. Вложения целевого фишинга отличаются от других форм целевого фишинга тем, что они используют вредоносное ПО, прикрепленное к электронным письмам. Все формы целевого фишинга представляют собой электронную социальную инженерию, нацеленную на конкретного человека, компанию или отрасль. В этом случае злоумышленники прикрепляют файлы к целевым фишинговым письмам и часто полагаются на действия пользователя для запуска вредоносного файла. Целевой фишинг также может включать в себя методы социальной инженерии, такие как позиционирование себя как надежного источника, например, старого делового партнера, или выдача себя за недавно уволенного сотрудника или отправка документов во время удаленной работы.

Существует множество вариантов вложения, таких как документы Microsoft Office, исполняемые файлы, jpg-файлы или архивированные файлы. При открытии вложения (и возможном щелчке) полезная нагрузка злоумышленника использует уязвимость или напрямую выполняется в системе пользователя вредоносный код. Текст фишингового электронного письма обычно пытается дать правдоподобную причину, по которой файл должен быть открыт, и может объяснить, как обойти системную защиты, чтобы сделать это, для повышения вероятности срабатывания данного вида атаки. Электронное письмо может также содержать инструкции о том, как расшифровать вложение, например, пароль zip-файла, чтобы избежать защиты границ электронной почты. Злоумышленники часто манипулируют расширениями файлов и иконками файлов, чтобы вложенные исполняемые файлы выглядели как файлы

документов, или файлы, использующие одно приложение, казались файлами для другого, что так же может повысить вероятность его исполнения пользователем.

Такой вектор атаки не гарантирует 100% срабатывания, однако опираясь на опыт многих компаний, даже крупных зарубежных, не говоря уже о небольших частных предприятиях он показывает себя как один из самых простых и эффективных в реализации. А значит может быть нацелен на массовую рассылку, что ожидаемо принесет «положительный» результат и множество пользователей столкнуться с проблемами разного характера связанными с работоспособностью их распределенной информационной системы.

Так же нельзя игнорировать и другие векторы проведения компьютерных атак, основанных на более сложных технических подходах. Но как показывает мировой опыт специалистов в сфере информационной безопасности, если способ в своей реализации стоит дешево и показывает свою состоятельность, то он обязательно привлечет внимание большого количества киберпреступников, в силу простоты воспроизведения и массовости исполнения. А это будет значить, что такой вектор угроз еще долго будет оставаться актуальным.

Так же метод отправки фишинговых писем не требует знания внутреннего устройства компании, что также делает его универсальным по отношению к любым предприятиям и государственным компаниям. Всю остальную работу будет выполнять сам вирус, что был зашит во вредоносный файл, который маскировался под обычный документ или архив.

Для рассматриваемого примера, в качестве атакуемого будет служить отдел коммерции компании Mobileye. Данный сегмент имеет свободный доступ к корпоративной почте, на которую периодически приходят письма от разных клиентов, подрядных организаций и других важных для компании партнеров. Это означает, что он находится в группе риска по отношению к данному

вектору атаки и его рассмотрение является обоснованным по перечисленным выше причинам.

2.3 Основные подходы к моделированию компьютерных атак

В настоящее время вопросы защиты распределенных информационных систем (РИС) от компьютерных атак приобретают все большее значение. Одним из наиболее важных направлений в этой сфере считается разработка методов и средств, позволяющих обнаружить, смоделировать, проанализировать и оценить факт начала и проведения атаки на систему.

Критическая информационная инфраструктура в широком смысле представляет собой набор независимых компьютеров, представляющийся их пользователям как единая система. РИС – это совокупность взаимодействующих друг с другом программных компонент, каждая из которых может рассматриваться как программный модуль или приложение, исполняемое в рамках отдельного процесса. Пользователи и приложения могут работать в системе независимо от того, где и когда происходит это взаимодействие. Но все КИИ должны иметь ряд характеристик, которые и являются отличительными чертами таких систем: сокрытие от конечных пользователей различий между компьютерами и способов связи между ними; относительно легкое масштабирование системы; невозможность отказа всей системы при выходе из строя некоторого отдельного элемента КИИ.

Так как под РИС подразумевают взаимосвязанный набор автономных компьютеров, процессов или процессоров, то их можно называть узлами КИИ. Чтобы быть взаимосвязанными, узлы должны иметь возможность обмениваться информацией, т. е. быть соединенными коммутирующей аппаратурой (коммуникационными модулями, каналами связи, концентраторами, межсетевыми экранами, шлюзами и т. д.).

В настоящее время не существует общепринятых формальных, математических или автоматизированных методов для моделирования,

оценивания и анализа безопасности системы, кроме наиболее простых, основанных на простых математических алгоритмах. В случае сложных информационных систем такие алгоритмы не применяются из-за больших затрат времени на их реализацию. Поэтому для оценивания безопасности систем используются методы, предполагающие экспертную оценку системы квалифицированными специалистами.

2.3.1 Математические методы моделирования компьютерных атак.

Для обеспечения более высоких уровней информационной безопасности CII и выявления ошибок, уязвимостей или незаявленной функциональности в ее программном обеспечении разрабатываются и создаются методы и инструменты, помогающие предотвратить нарушения безопасности системы. Именно на этапе разработки системы большое внимание уделяется поиску и исследованию уязвимостей.

Существуют методики и программные средства, позволяющие устранить ошибки при работе с языками или внешними интерфейсами (в частности, Microsoft Prefast), а также большое количество ошибок (PEACH и спайки), связанных с логикой обработки данных, реализацией протокола, и т.п. Однако многие автоматизированные методы позволяют оценить защищенность системы только в простых случаях. Именно по этим причинам область моделирования компьютерных атак изучается более 10 лет.

Много научных работ посвящено моделированию компьютерных атак на основе различных математических моделей, каждая из которых имеет свои преимущества и недостатки. Перспективным направлением в области моделирования атак на КИИ является теория автоматов. Теория автоматов может простейшим образом описать атаку компьютера на систему, но из-за информации о состоянии системы и неполноты информации расчета передачи автомата непосредственная реализация этой модели для большинства реальных информационных систем невозможна, а два Ограничения недопустимы для

моделирования компьютерных атак на CII, поскольку при таком математическом подходе переходы из одного состояния в другое зависят от случайных входных сигналов или последовательности предыдущих состояний.

В результате аналитическое представление функций выходов автомата для КИИ в общем случае невозможно [9]. Специалисты по информационной безопасности предлагают модель сетевой атаки и алгоритм обнаружения угроз сетевой безопасности. Модель предназначена для анализа и прогнозирования изменения уровней информационной безопасности системы на основе событий, происходящих в сети. С помощью нескольких экземпляров автоматов кибератак можно предсказать поведение злоумышленника на техническом уровне и предсказать наиболее вероятный следующий этап атаки. Многие экземпляры могут иметь разные состояния и описывать действия разных узлов сети. В предлагаемом методе используются диаграммы состояний автоматов и вероятности переходов. Интересно, что при таком подходе в разработанную модель вводится понятие «период актуальности» для событий ИБ. Например, анализ события отправки запроса по определенному протоколу имеет смысл только при получении ответа. Таким образом, список событий информационной безопасности представляется в виде набора кортежей (источник, получатель, тип события, тип события отключения, время жизни). Такой подход несколько упрощает задачу вероятностных автоматов и может быть использован для небольших распределенных систем. В общем случае математические методы для моделирования компьютерных атак можно разделить на четыре больших класса, представленных на рис. 1.

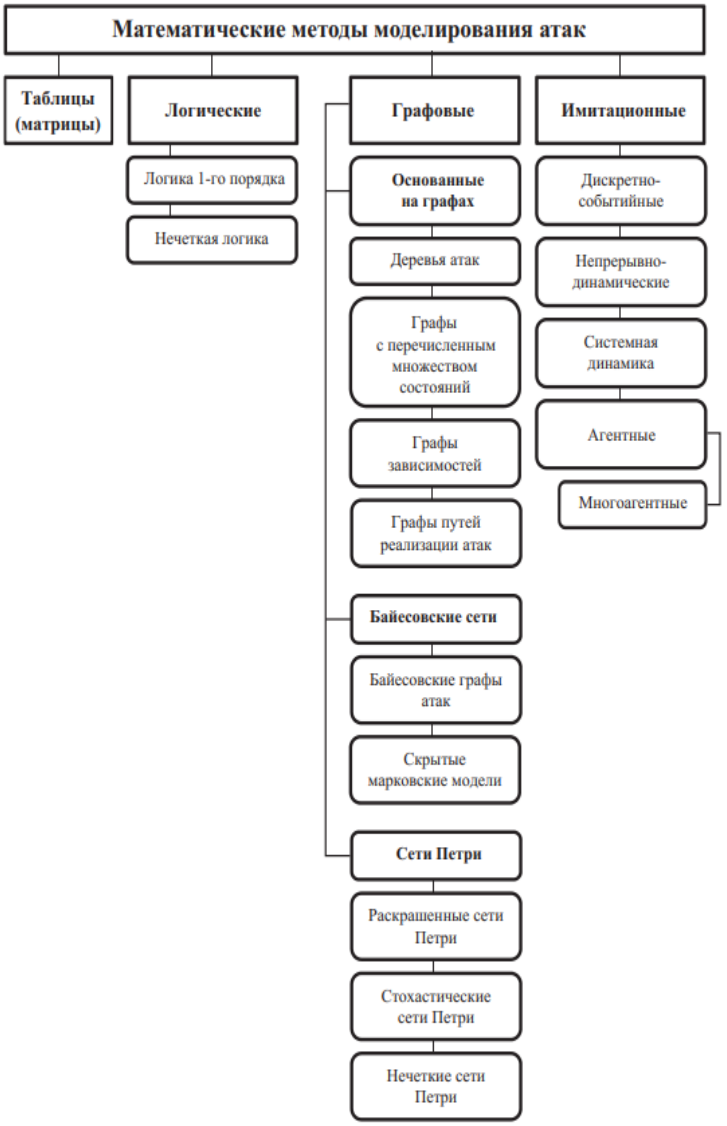

Рисунок 1. Математические методы для моделирования компьютерных атак.

Табличные (матричные) методы моделирования компьютерных атак являются наиболее простыми в реализации. Но такие модели трудно использовать при моделировании атак на системы, в которых большое количество объектов, субъектов и связей между ними. Под объектами подразумеваются инциденты информационной безопасности, а субъекты – нарушители. Также такие типы моделей не совсем подходят для анализа циклических атак. Тем не менее подобные модели удобны в тех случаях, когда информация (входные данные модели) представляет собой набор малосвязанных друг с другом инцидентов или правил обнаружения атак. Этот метод может

применяться для моделирования атак в небольших информационных системах (ИС).

2.3.2 Применение марковских процессов для целей обеспечения информационной безопасности

Рассмотрение Марковских процессов интересует большое количество людей, занимающихся моделированием систем в области информационной безопасности. Этот метод позволяет строить системы любой сложности, за счет простоты описания вероятностных переходов из одного условия в другое, так как перейдя из состояния в состояние, она не обязана учитывать предыдущее. Такой подход позволяет применять его к моделированию различных угроз к распределенным информационным системам практически любого объема.

Для рассмотрения этого метода на примере, можно воспользоваться моделью поведения нарушителя по реализации внутренних угроз, намерением которого является - преодоление защищаемых средствами безопасности основных постулатов информационной безопасности, а именно: конфиденциальности, целостности, доступности. ИС в результате воздействия нарушителя переходит из состояния в состояние только в фиксированные моменты времени T = {t 1, t2, …, t k}, которые являются этапами Марковского процесса. По тем состояниям, в которых может находиться ИС в различные моменты времени, составляется матрица переходных вероятностей системы и строится граф состояний при воздействии нарушителя. Пример подобного графа представлен на рис. 2.

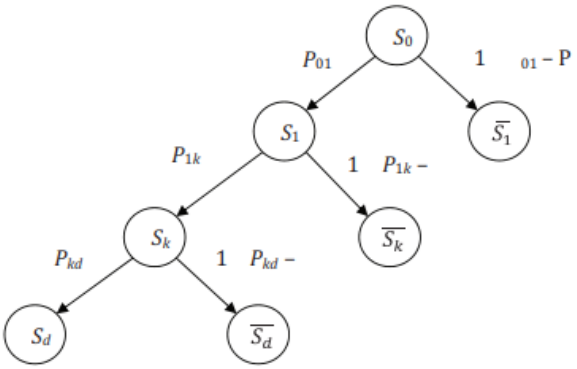

Рисунок 2. Граф состояний ИС

Используя его, можно получить аналитические выражения для определения вероятностей благополучного и неблагополучного исхода при воздействии на ИС различных нарушителей.

Таким образом, метод моделирования компьютерных атак на основе Марковских процессов является наиболее простым и в то же время наиболее эффективным для РИС [15]. Его применение не требует построения больших таблиц и матриц, как в табличных методах, или знания всех предыдущих состояний, как в методах вероятностных автоматов и нейронных сетях.

2.3.3 Применение метода моделирования реакции распределенной информационной системы на компьютерные атаки, воспроизводимые на стенде

Наиболее подходящим методом для моделирования угрозы КИИ в данной работе будет являться имитирование реакции информационной системы посредством проведения компьютерной атаки на виртуальную среду. Данный подход в полной мере может показать, как система будет себя вести при реализации вектора атаки выбранного из базы Miter Attack, что позволит обеспечить наибольшее соответствие описанному выше методу «Фишинг: Прикрепление целевого фишинга». Это позволит точнее повлиять выявление слабых мест информационной системы, а также предоставит наглядную информацию, которую можно будет использовать для анализа специалисту по информационной безопасности.

Для реализации этого метода необходимо определить исходные данные. В качестве исходных данных следует определить три множества, описывающие модель распределенной информационной системы с точки зрения возможной реализации компьютерной атаки.

Множество уязвимостей, характерных для Mobileye. Для данного примера была выбранная уязвимость «Фишинг: Прикрепление целевого фишинга». То

есть распространение вредоносных программ посредством отправки писем, содержащих скрытые угрозы.

Множество угроз было подобрано исходя из наиболее актуальных на сегодняшний день вредоносных программ. А именно вирус Шифровальщик и Сетевой червь.

Под множеством нарушителей будет подразумеваться пользователь информационной системы, не осведомленный о базовых принципах информационной безопасности, либо сознательно опустивший данные правила, в силу коммерческой или личной заинтересованности в нарушении имиджа или финансовых показателях организации, в которой он осуществляет свою деятельность.

Компьютерной атакой будем считать любое действие со стороны нарушителя, которое повлекло сбои в работе отдела.

2.4 Моделирование реакции распределенной информационной системы на компьютерные атаки

Моделирование как процесс показывает реакцию той или иной системы в изменяющихся для нее условиях. Моделирование распределенной информационной системы позволяет оценить ее степень сопротивляемости проводимым деструктивным действиям, в данном случае атаки.

Результаты моделирования помогут экспертам точнее определить то, насколько система становится более устойчивой к внешним атакам с учетом применяемых инструментов защиты. Так же метод моделирования реакции распределенной информационной системы позволит на примере узкого сегмента сети оценить его реакцию и даст возможность определить какой из инструментов защиты показал себя наилучшим образом.

2.4.1 Подготовка стенда.

Моделирование и отработка возможных угроз защищаемой информации, атак на информационные ресурсы и реакций средств защиты информации на данные ситуации достигается путем разработки и практической реализации имитационного стенда (ИС) для моделирования действий нарушителя в защищенной информационно-телекоммуникационной инфраструктуре на базе современного оборудования. При моделировании должны учитываться новейшие способы хранения, обработки и передачи информации, способы и методы реализации угроз информации и противодействия им [8].

При проектировании и создании ИС должно учитываться все разнообразие существующих и потенциальных угроз безопасности информации, их разнонаправленность и наличие множества различных вариантов и средств их реализации. Стенд должен давать возможность моделировать указанные сценарии.

2.4.2 Описание стенда.

Стенд будет моделировать реально существующий отдел коммерции. Так как данный отдел наиболее часто принимает на свою электронную почту сообщения с различными рода предложениями, что уже потенциально говорит о заинтересованности его сотрудников в тщательном изучении присылаемых писем. Так же, так как этот отдел никак не связан с технической стороной процесса разработки или другой технической деятельности, то будем полагать, что сотрудники не имеют представления о базовых принципах информационной безопасности. Что так же в свою очередь делает его потенциально уязвимым перед внешними угрозами.

Техническое описание стенда и используемые инструменты в реализации моделирования атак будут подобраны исходя из описанных в 1 главе особенностей распределенной системы Mobileye.

В качестве основного инструмента для создания среды тестирования будет использоваться программа VMware Workstation. Данный инструмент является оптимальным для данной задачи, так как позволяет реализовать модель отдела коммерции с большой точностью, за счет гибкой системы настроек самих виртуальных машин. Для реализации будет воссоздано 2 виртуальные машины, каждая из которых будет обрабатывать информацию не зависимо друг от друга, но при этом они будут связаны в 1 локальную сеть и иметь базы данных пользователей в виде таблицы csv.

За основу операционной системы для создания самих виртуальных машин будет взята Windows 10. Она является наиболее распространенной в коммерческом секторе, а также более дружелюбной для пользователя не имеющим глубоких познаний в технической части.

Почтовым сервисом, принимающим письма будет выступать обычная почта от google – gmail. Так как она является достаточной для воссоздания описываемого сценария. Почтовым сервисом с которого будет отправляться письмо будет yandex почта. Также будет использован Яндекс диск, для сокрытия файла в общую папку.

2.4.3 Реализация исследования

На данном этапе будет проходить подготовка к созданию виртуальной машины. Необходимо задать технические параметры при ее создании. Сами значения не будут играть большой роли для исследования, поэтому можно опустить данный этап.

Нам понадобится преобразовать исходные вирусы в файлы с другим расширением, например, jpg чтобы у пользователя, который будет получать письмо не возникло подозрений. Для реализации этой задачи потребуется HEX редактор, для примера будет использован HxD. Чтобы преобразовать исполняемы файл в картинку необходимо для начала поместить исходный вирус в архив, что продемонстрированно на рисунках 3 и 4.

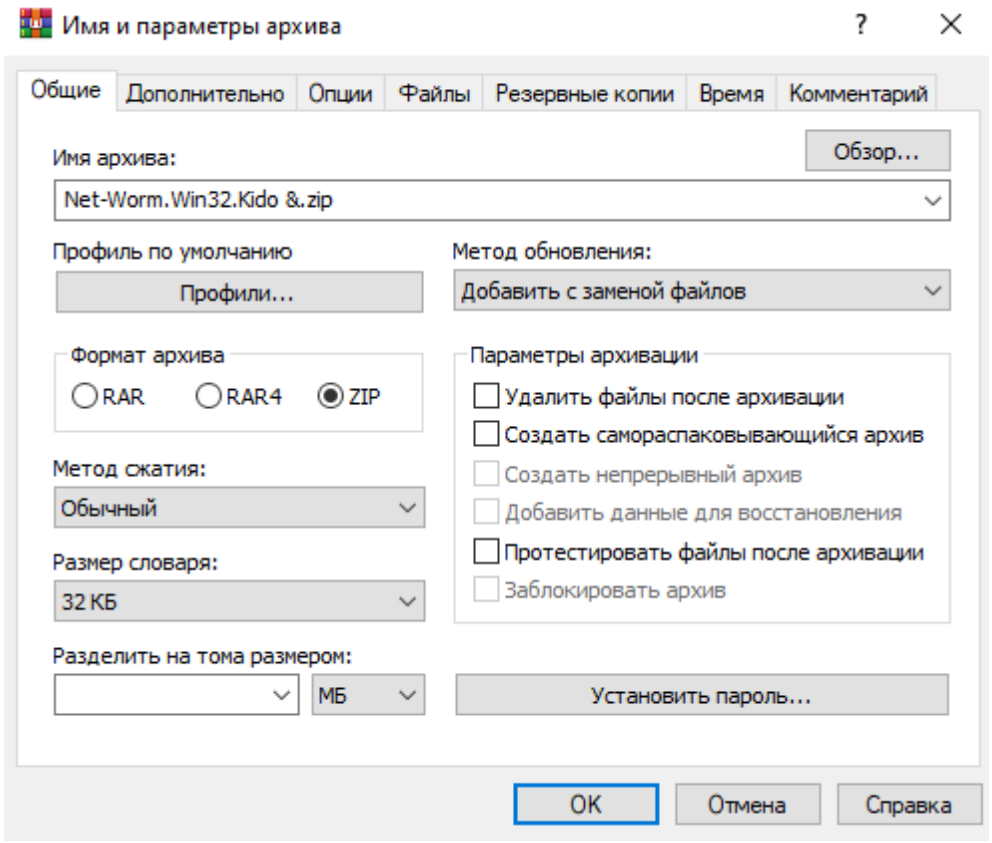

Рисунок 3. Архивирование сетевого червя.

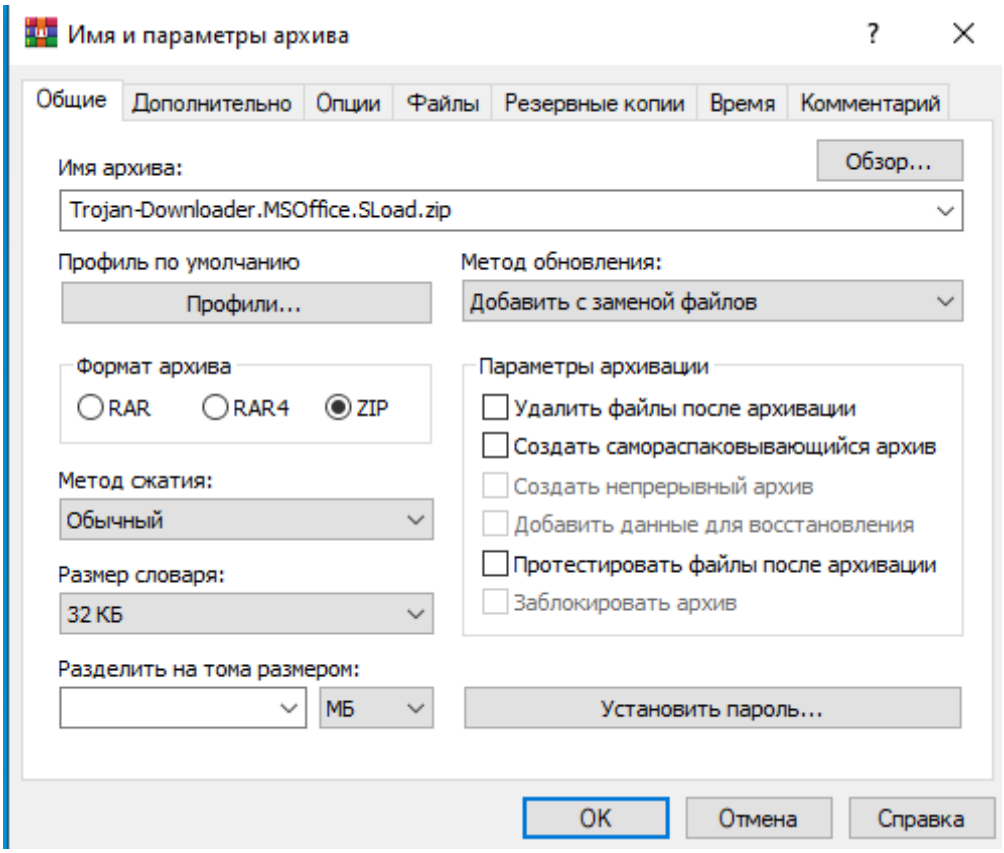

Рисунок 4. Архивирование вируса Шифровальщика.

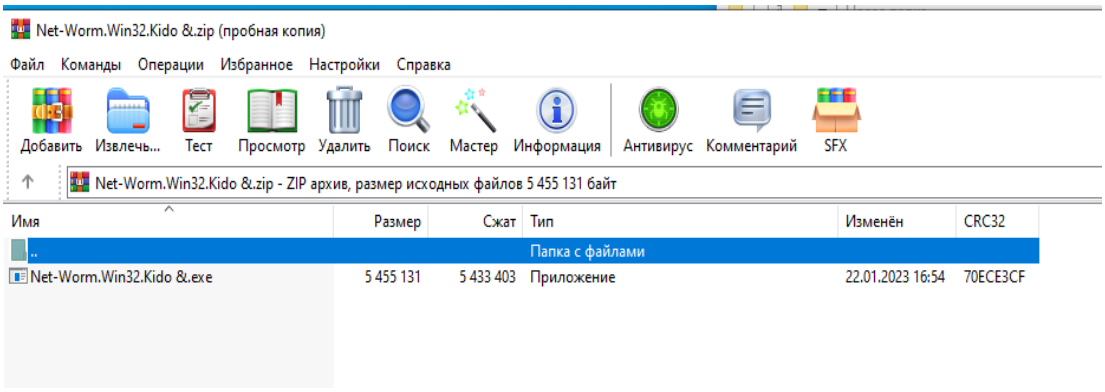

Рис.5 Вирус Сетевой червь в архиве

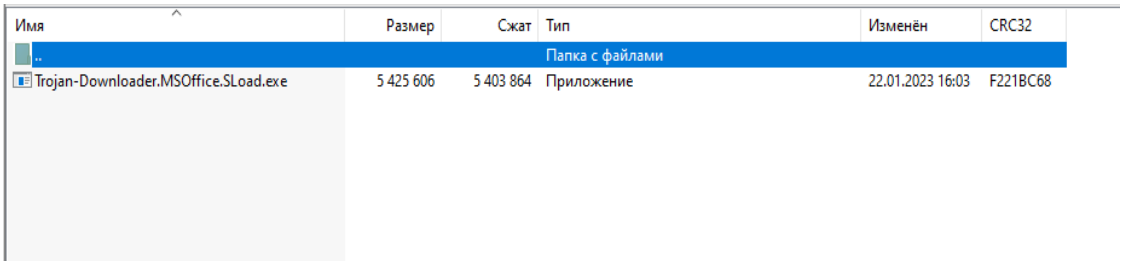

Рисунок 6. Вирус шифровальщик в архиве

После этого поместим эти архивы в папку где находится сам HEX редактор. Далее один из архивов перетащим на иконку редактора, в следствии чего у нас откроется окно программы с содержимым архива, представленного в виде бинарного кода, рисунок 7.

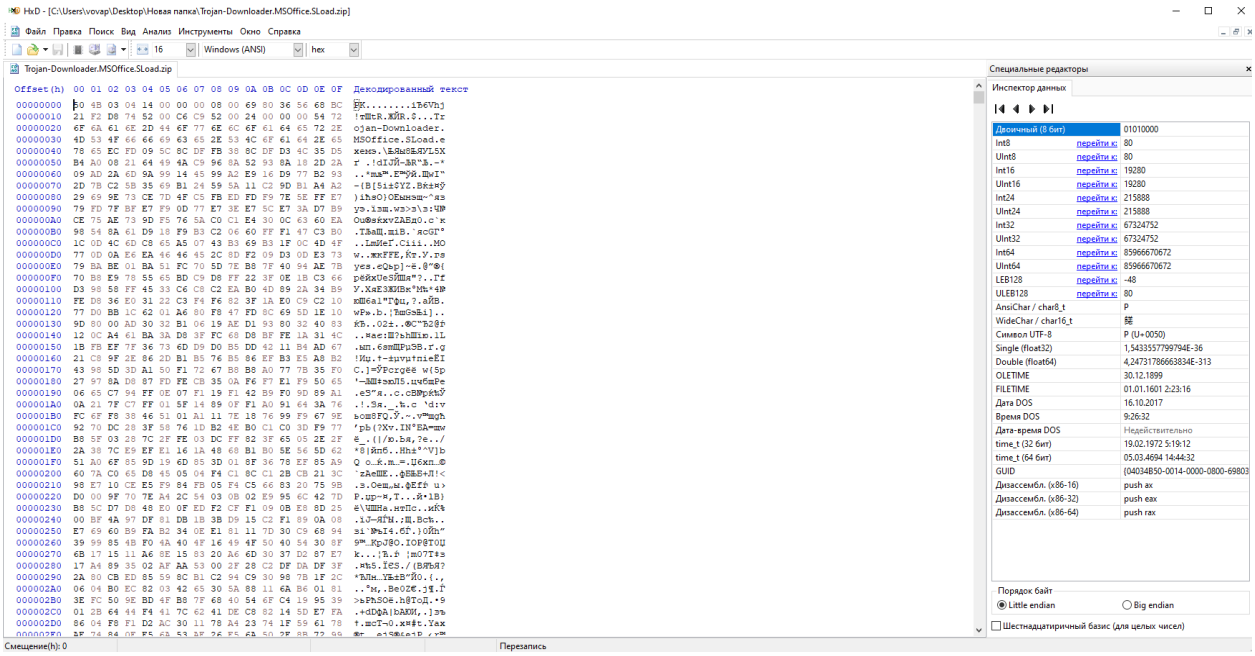

Рисунок 7. Содержимое архива.

Чтобы поменять расширение exe файла на jpg, мы должны найти соответствующее значение в самом редакторе. Для этого можно воспользоваться поиском и вбить исходное расширение – exe. После этого мы увидим, что в данных отобразятся 2 значения, одно на самом верху, другое внизу. Чтобы изменить расширение, нужно изменить нижний параметр. Процесс работы изображен на рисунках 9 и 10.

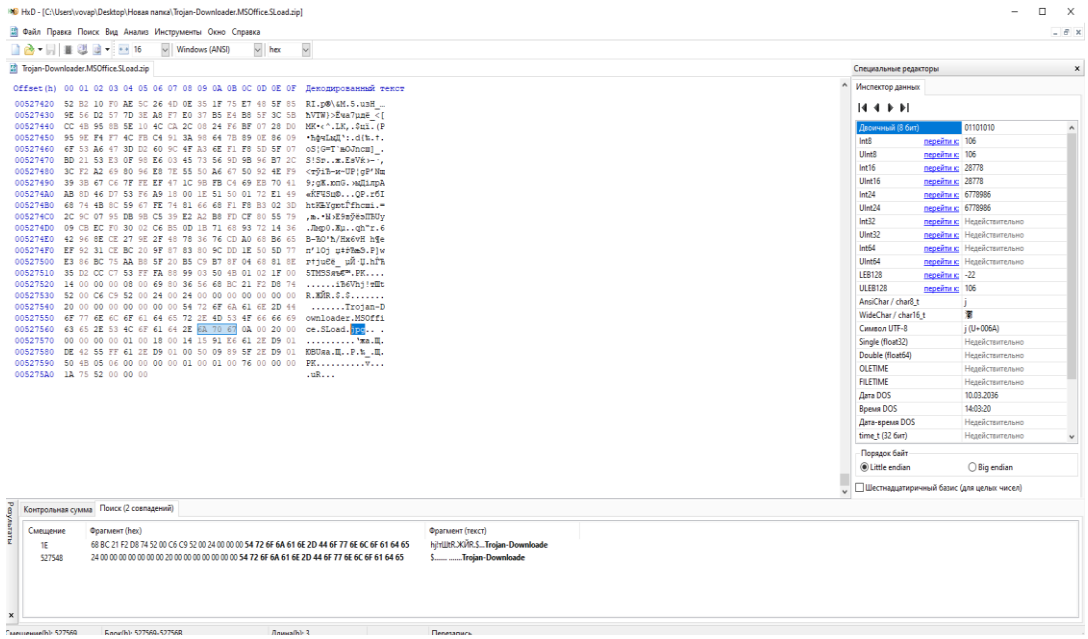

Рисунок 11. Изменение расширения шифровальщика.

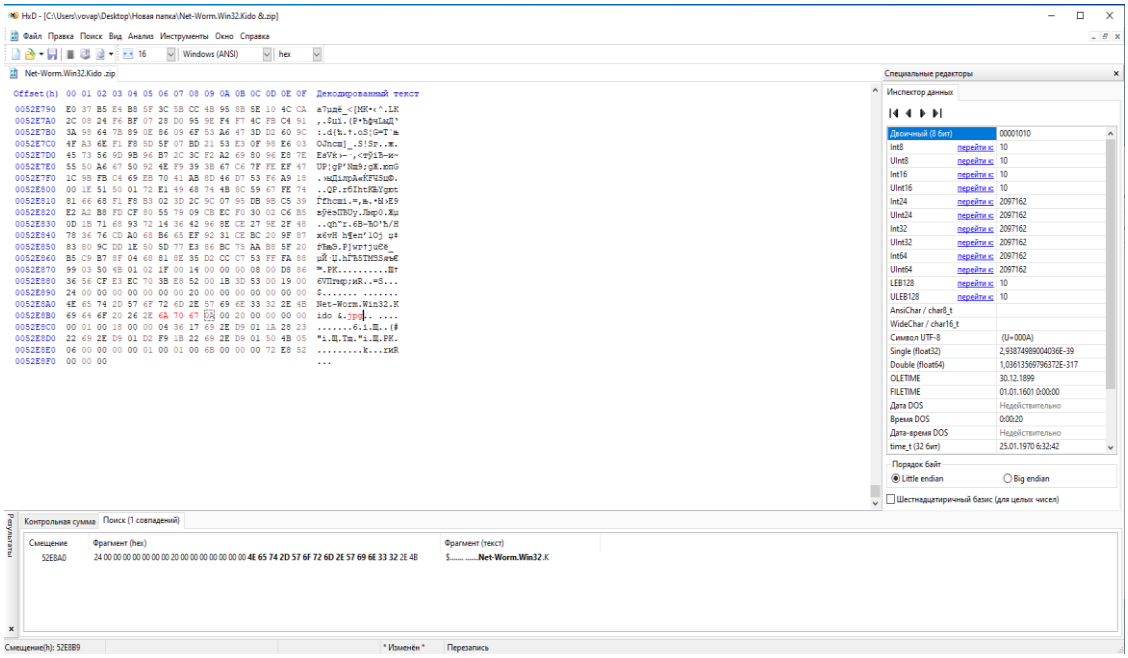

Рисунок 12. Изменение расширения Сетевого червя.

После сохранения изменений мы увидим, что у содержимого архивов, куда мы помещали угрозы, поменялось расширение, рис.8, рис.9.

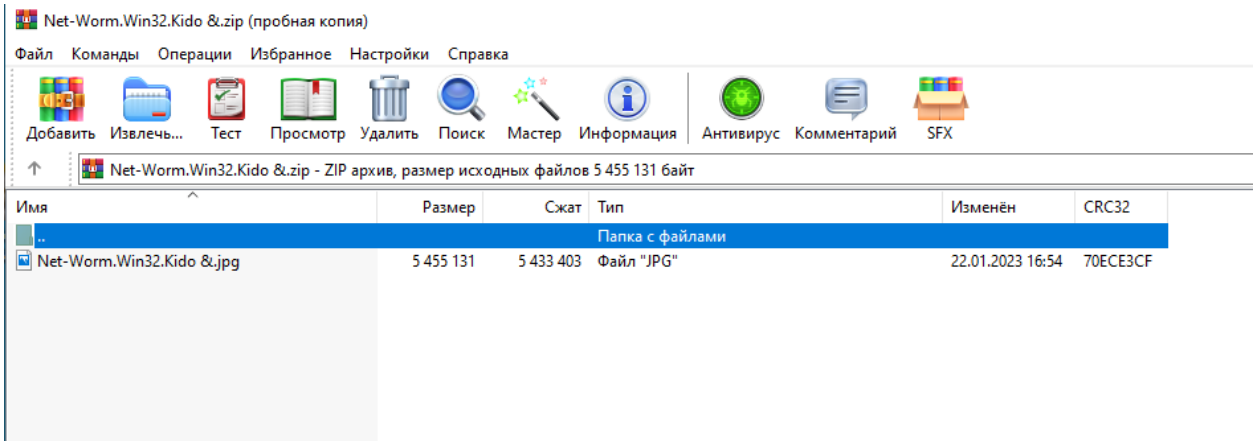

Рисунок 13. Вирус сетевой червь с новым расширением

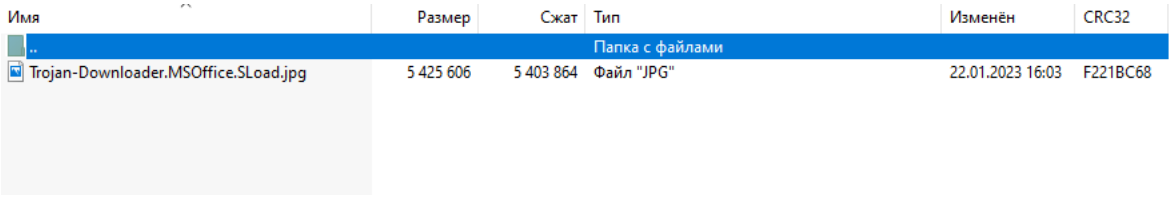

Рисунок 14. Шифровальщик с новым расширением

Сравнивая рисунки 5,6 и 13,14 можно заметить, что преобразование расширения файла прошло успешно.

Подготовив исходные данные для моделирования атаки, можно приступить к следующему этапу – рассылке вредоносного сообщения. Для отправки сообщения не принципиален почтовый сервис или клиент, поэтому, были выбраны сервисы яндекс почта и гугл почта, как самые популярные.

Перед отправкой письма, необходимо провести небольшое исследование, чтобы понять какие сообщения могут вызвать больший интерес у получателя. В данном примере было решено использовать сообщение, включающее в себя информацию о скорой премии.

Так же необходимо обратить внимание на то, что на сегодняшний день, компании, занимающиеся развитием своих почтовых клиентов тоже осведомлены об атаке через фишинговые письма. По этой причине загружаемый как вложение - файл, содержащий вирус не будет отправлен, а

отправитель получит ответное письмо от технической поддержки, с кодом ошибки. Посмотрев код ошибки, можно будет понять, что анализатор вирусов, встроенный в почтовую систему обнаружил вирусную сигнатуру и отказал в отправке. По этой причине подход был изменен.

Для отправки письма с вредоносом, перед написанием самого письма был использован сервис яндекс диск. В нем была создана папка под названием “Важно”, в которую был помещен вирус, с заранее измененным названием, на то, которое заинтересует получателя, рисунок 15.

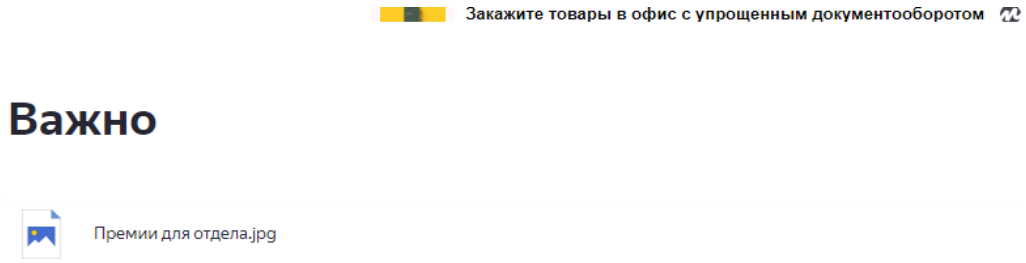

Рисунок 15. Вложенный в сетевое хранилище вирус.

После чего был обеспечен общий доступ к данной папке. И теперь ссылку на нее можно без проблем использовать для написания письма, сократив ее, либо изменив под подходящее по смыслу письма.

На принимающей стороне было получено письмо со следующим содержанием, Рисунок 16

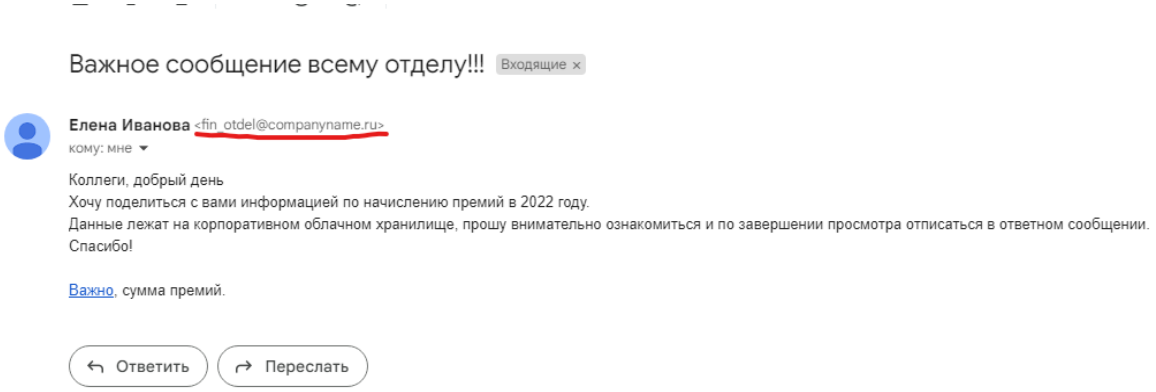

Рисунок 16. Пример фишингово письма

Теперь мы можем рассмотреть 2 варианта развития событий. Первый подразумевает под собой успешную эксплуатацию обеих угроз. Второй же наоборот, показывает, как системе удалось противостоять вирусам, несмотря на то, что они проникли в систему.

В первом случае, когда на машинах установлены старые антивирусные базы, либо по какой-то причине совсем не стоят системы защиты, мы можем увидеть следующее проявление вирусов:

1. Шифровальщик. Попадая на компьютер жертвы, он моментально производит сканирование имеющихся файлов, для их шифрации, так же он имеет возможность повреждения файла, что помешает его открытию.

Пример зашифрованного и поврежденного файла можно наблюдать на рисунках 17,18.

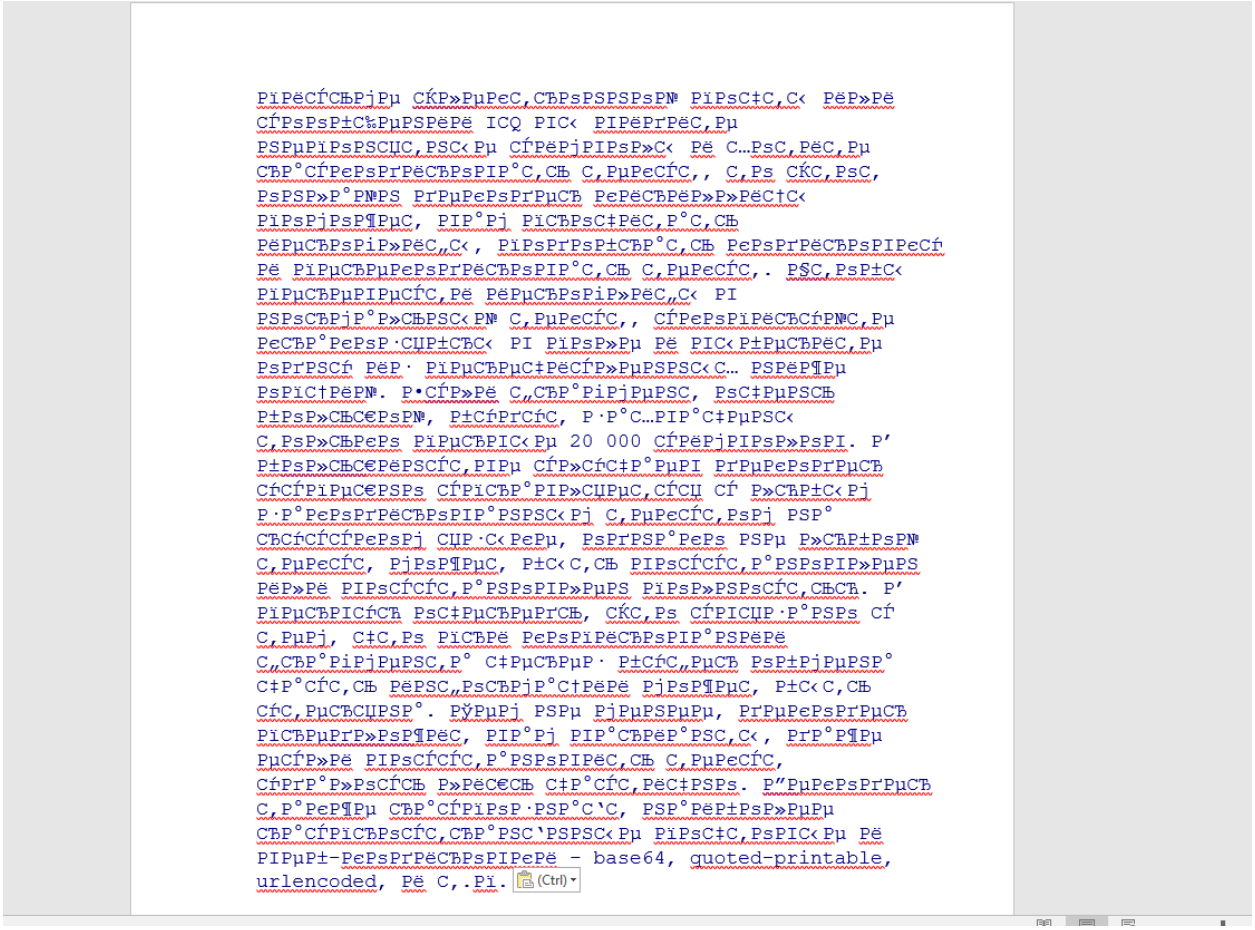

Рисунок 17. Зашифрованный фрагмент текста документа

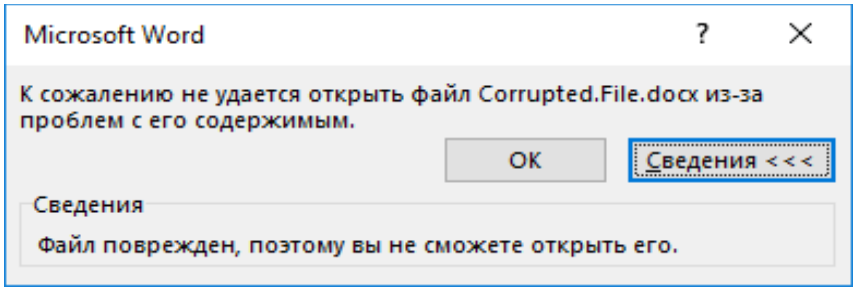

Рисунок 18. Повреждение документа

2. Сетевой червь. Проявление данной угрозы так же можно заметить невооруженным глазом. Система начинает вести себя нестабильно, выдавать ошибки и перезагружаться. Что бы продемонстрировать

наличие этого вируса на компьютере, есть рисунок 19.

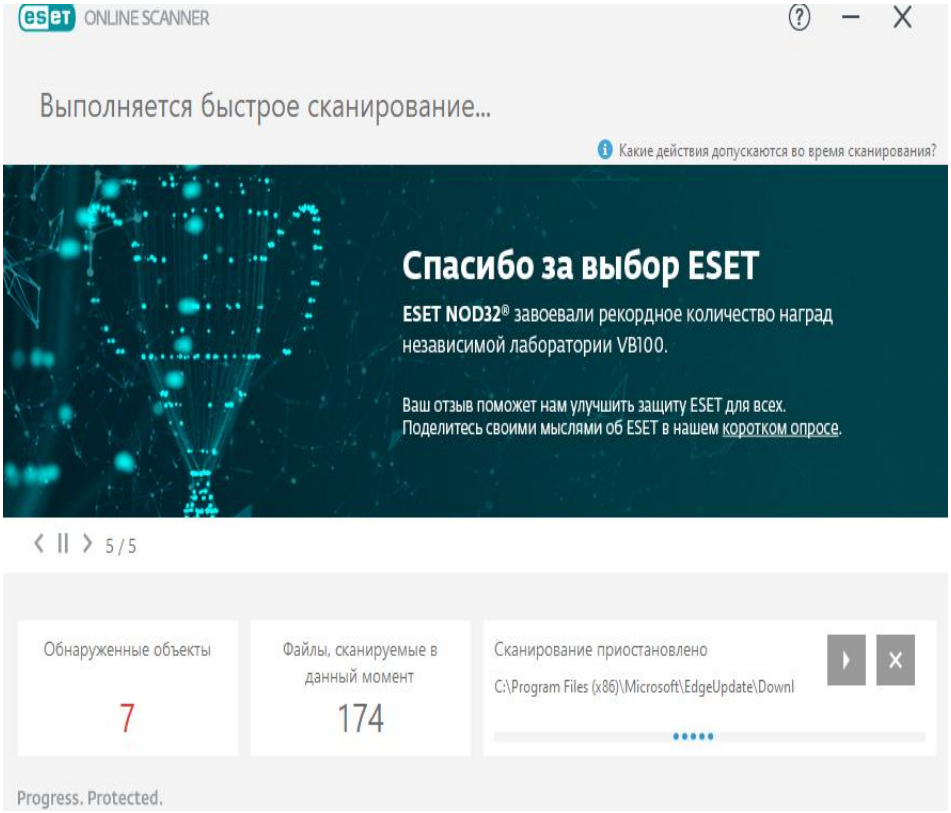

Рисунок 19. Обнаружение угроз, связанных с появлением сетевого червя.

Во втором случае, будет рассмотрен сценарий, когда угрозы не были проэксплуатированны успешно. Для этого понадобилось установить современный антивирус, с возможностью обновления сигнатур баз данных. При отправке сообщений с разными вирусными файлами и их скачиванием, антивирус реагировал незамедлительно, что позволило избежать последствий, приведенных в примере выше. После анализа системы, антивирус смог распознать встроенные в картинку угрозы предложил рекомендации по их

устранению, рисунок 20.

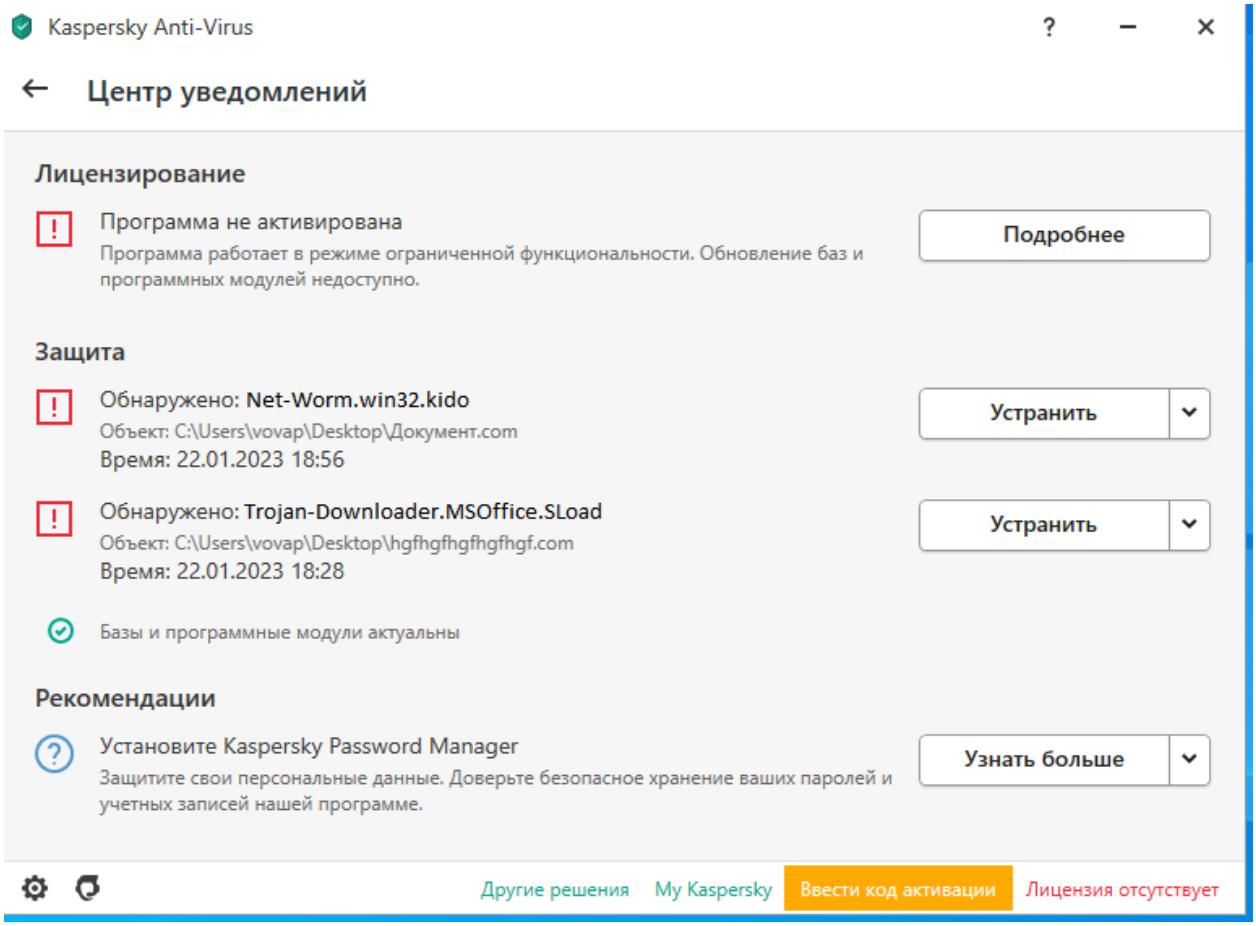

Рисунок 20. Обнаруженные угрозы

Вывод по 2 главе:

Подводя итоги проведенного моделирования, можно сделать промежуточные выводы. А именно, почтовые системы не стоят на месте и не позволяют отправлять вирус напрямую, даже если он зашит в картинку или другой файл. Но несмотря на это, те же самые сервисы позволяют использовать свои облачные хранилища в качестве места для хранения вирусов и не проводят анализ сигнатур. Это примечательно по той причине, что вложенный в папку с открытым доступом вирус может свободно распространяться в сети интернет. Что может повлечь за собой массовое заражение компьютеров, при должном подходе при грамотном подходе к социальной инженерии.

ГЛАВА 3. ПРОВЕДЕНИЕ РАСЧЕТОВ ПО СОБРАННЫМ ДАННЫМ

3.1 Сбор данных

В данном разделе будет проанализирован проведенный опрос специалистов по информационной безопасности. Целью опроса будет служить получение достаточного количества оценок, для проведения исследования. Будут сформулированы однозначно поставленные вопросы, которые помогут измерить уровень доверительного интервала, который покажет, как менялась достоверность оцениваемой системы до и после применения стенда. Результаты полученные в ходе проведения расчетов можно будет трактовать как истинные, исходя из высокой репрезентативности исходной генеральной совокупности.

Для получения численного значения оценки проделанной работы необходимо подготовить исходные данные. В качестве источника для получения репрезентативной выборки была составлена Яндекс форма. Она включает в себя необходимы перечень вопросов и ознакомительной информации, для точного ответа на них.

В качестве экспертов, отвечающих на вопросы, были выбраны специалисты по информационной безопасности. Группа была подобрана исходя из их опыта и степени осведомленности о проводимом исследовании. Что на выходе помогло получить честные данные. Главным критерием при отборе кандидата для проводимого исследования была его заинтересованность в данном опросе, что помогло отсеять нерелевантные значения, которые не поспособствовали бы точному измерению. После проведения опроса и отсеивания не заполненных до конца анкет, удалось собрать 30 полностью готовых ответов.

Данными которыми заполняли эксперты, являлись ответы на следующие вопросы:

- Как вы оцените вероятность реализации угрозы "Червь" в системе Mobileye?

- Как вы оцените вероятность реализации угрозы "Шифровальщик" в системе Mobileye?
- Как вы оцените вероятность реализации угрозы "Червь", в системе Mobileye, при условии, что этот вирус на стенде проэксплуатирован успешно?
- Как вы оцените вероятность реализации угрозы "Шифровальщик", в системе Mobileye, при условии, что этот вирус на стенде проэксплуатирован успешно?
- Как вы оцените вероятность реализации угрозы "Червь", в системе Mobileye, при условии, что этот вирус на стенде не был проэксплуатирован успешно?
- Как вы оцените вероятность реализации угрозы "Червь", в системе Mobileye, при условии, что этот вирус на стенде не был проэксплуатирован успешно?

Каждый из этих вопросов имел прямое отношение к проводимому исследованию и давал возможность оценить вероятность того или иного события. Результаты опроса представлены на рисунке 22.

Какой вари	Как вы оцените вероятность реал	Как вы оцените вероятность ре	Как вы оцените вероятность реализ	Как вы оцените вероятность ре	Как вы оцените вероятность реа	Как вы оцените вероятность реа
1	0,18	0,19	0,7	0,74	0,1	0,1
2	0,8	0,9	0,9	0,9	0,1	0,1
3	0,19	0,1	0,95	0,83	0,11	0,1
4	0,73	0,74	0,85	0,91	0,5	0,51
5	0,18	0,2	0,8	0,8	0,15	0,16
6	0,28	0,15	0,88	0,86	0,23	0,12
7	0,41	0,4	0,79	0,78	0,35	0,33
8	0,96	0,98	0,95	0,97	0,5	0,5
9	0,19	0,26	0,64	0,66	0,11	0,17
10	0,18	0,14	0,81	0,88	0,12	0,13
11	0,29	0,14	0,77	0,63	0,25	0,1
12	0,2	0,15	0,81	0,89	0,16	0,11
13	0,11	0,09	0,87	0,65	0,1	0,08
14	0	0	1	1	0	0
15	0,42	0,45	0,98	0,87	0,2	0,23
16	0,17	0,21	0,87	0,97	0,13	0,19
17	0,26	0,15	0,63	0,65	0,17	0,12
18	0,12	0,09	0,45	0,37	0,07	0,03
19	0,27	0,25	0,78	0,73	0,27	0,22
20	0	0	1	1	0	0
21	0,48	0,5	0,87	0,87	0,35	0,35
22	0,18	0,13	0,67	0,58	0,12	0,1
23	0,29	0,2	0,65	0,6	0,13	0,17
24	0,25	0,25	0,8	0,8	0,1	0,1
25	0,7	0,78	0,9	0,9	0,15	0,14
26	0,1	0,1	0,76	0,76	0,1	0,1
27	0,15	0,17	0,68	0,7	0,12	0,14
28	0,34	0,35	0,67	0,64	0,3	0,3
29	0,2	0,2	0,6	0,6	0,13	0,11
30	0,15	0,15	0,68	0,68	0,1	0,12

Рисунок 21. Результаты опроса

По завершении опроса, был начат следующий этап – проведение статистических расчетов.

3.2 Проведение расчетов на основании собранных данных

Каждое значение что было получено, занесено в таблицу. Для большей наглядности собранные данные так же были преобразованы в точечную диаграмму.

Точечная диаграмма позволяет наглядно ценить разброс полученных значений. Вопросы и ответы по ним:

1. Как вы оцените вероятность реализации угрозы "Червь" в системе Mobileye? Рисунок 23.

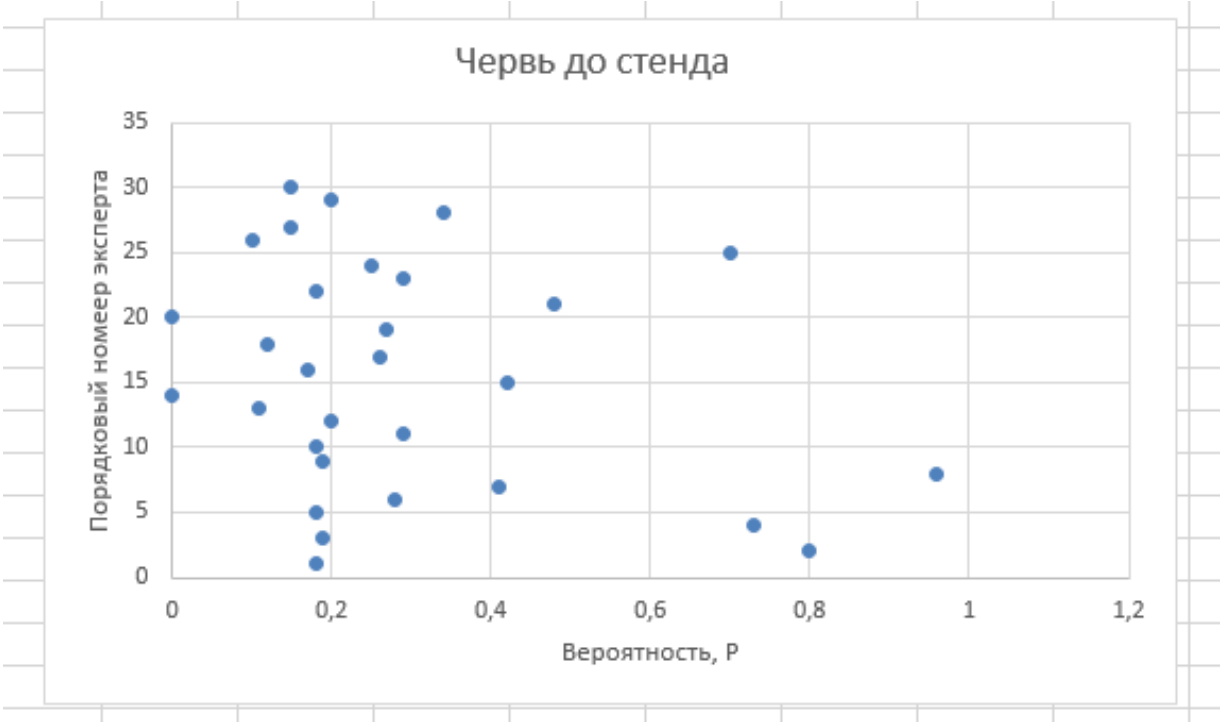

Рисунок 23. Точечная диаграмма

2. Как вы оцените вероятность реализации угрозы "Шифровальщик" в системе Mobileye? Рисунок 24.

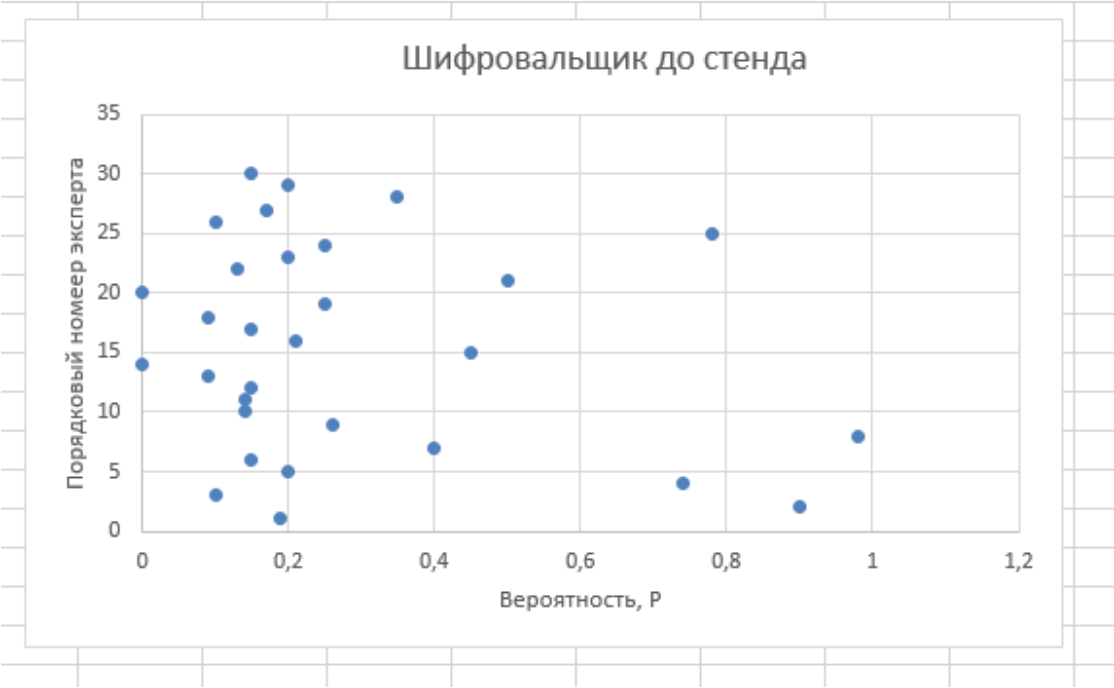

Рисунок 24. Точечная диаграмма

3. Как вы оцените вероятность реализации угрозы "Червь", в системе Mobileye, при условии, что этот вирус на стенде проэксплуатирован успешно? Рисунок 25.

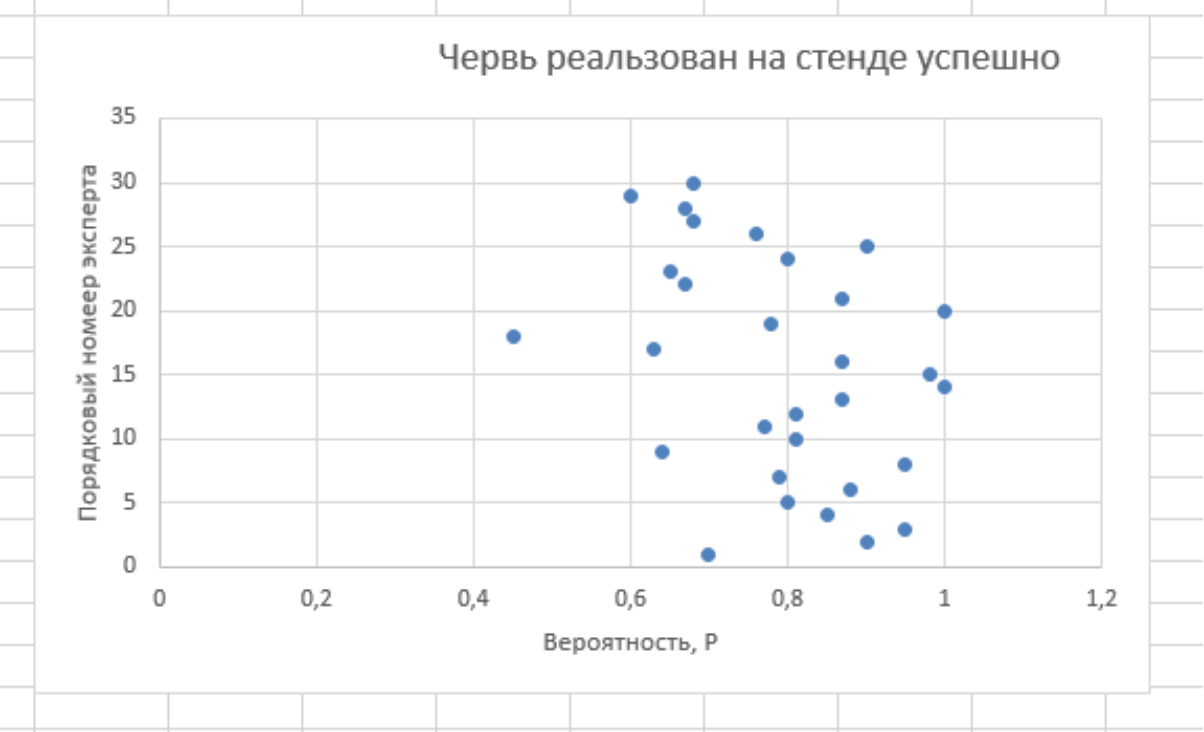

Рисунок 25. Точечная диаграмма

4. Как вы оцените вероятность реализации угрозы "Шифровальщик", в системе Mobileye, при условии, что этот вирус на стенде проэксплуатирован успешно? Рисунок 26.

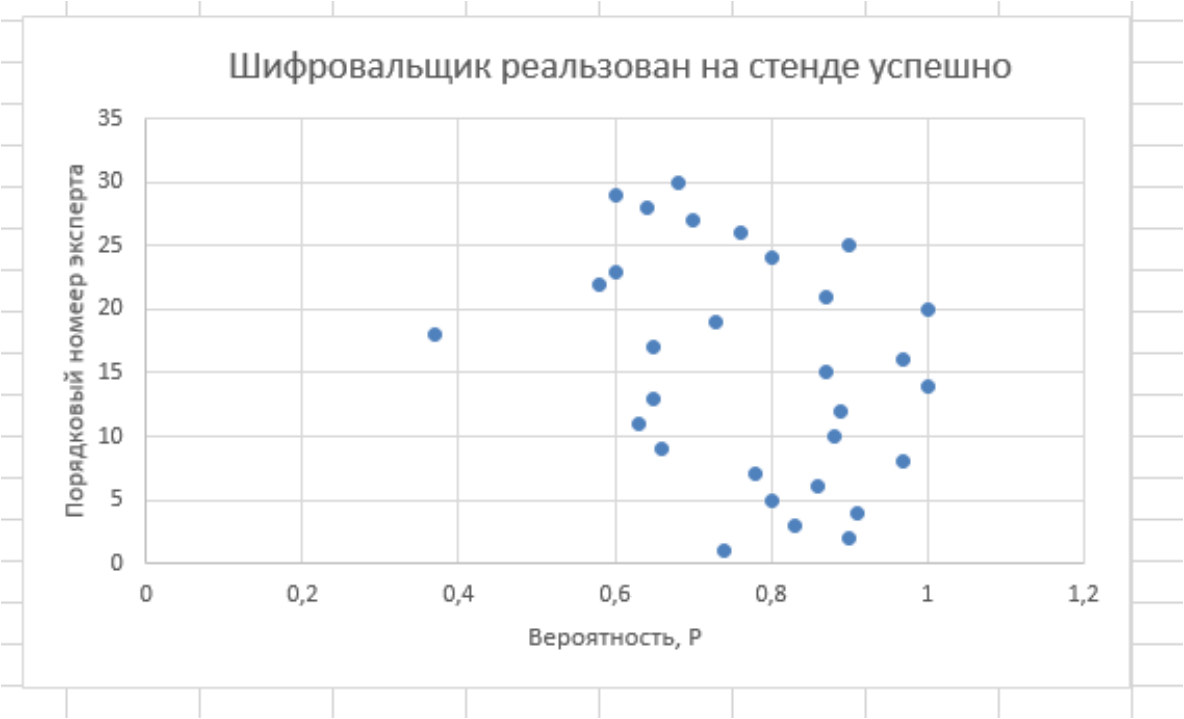

Рисунок 26. Точечная диаграмма

5. Как вы оцените вероятность реализации угрозы "Червь", в системе Mobileye, при условии, что этот вирус на стенде не был проэксплуатирован успешно? Рисунок 27.

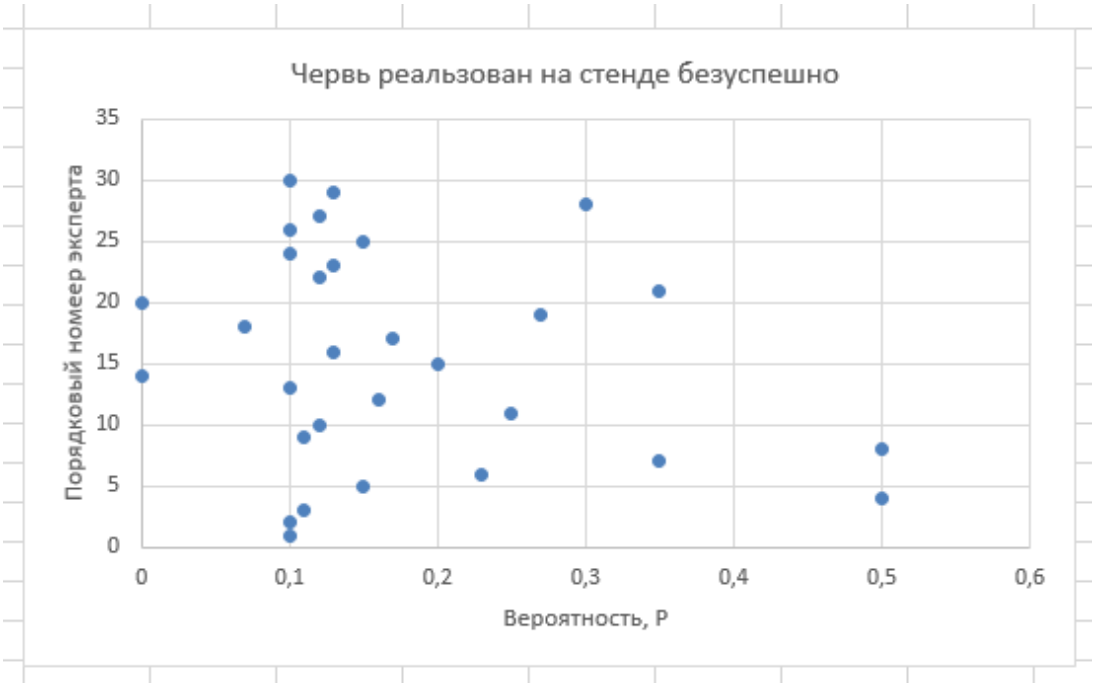

Рис. 27 Точечная диаграмма

6. Как вы оцените вероятность реализации угрозы "Червь", в системе Mobileye, при условии, что этот вирус на стенде не был проэксплуатирован успешно? Рисунок 28

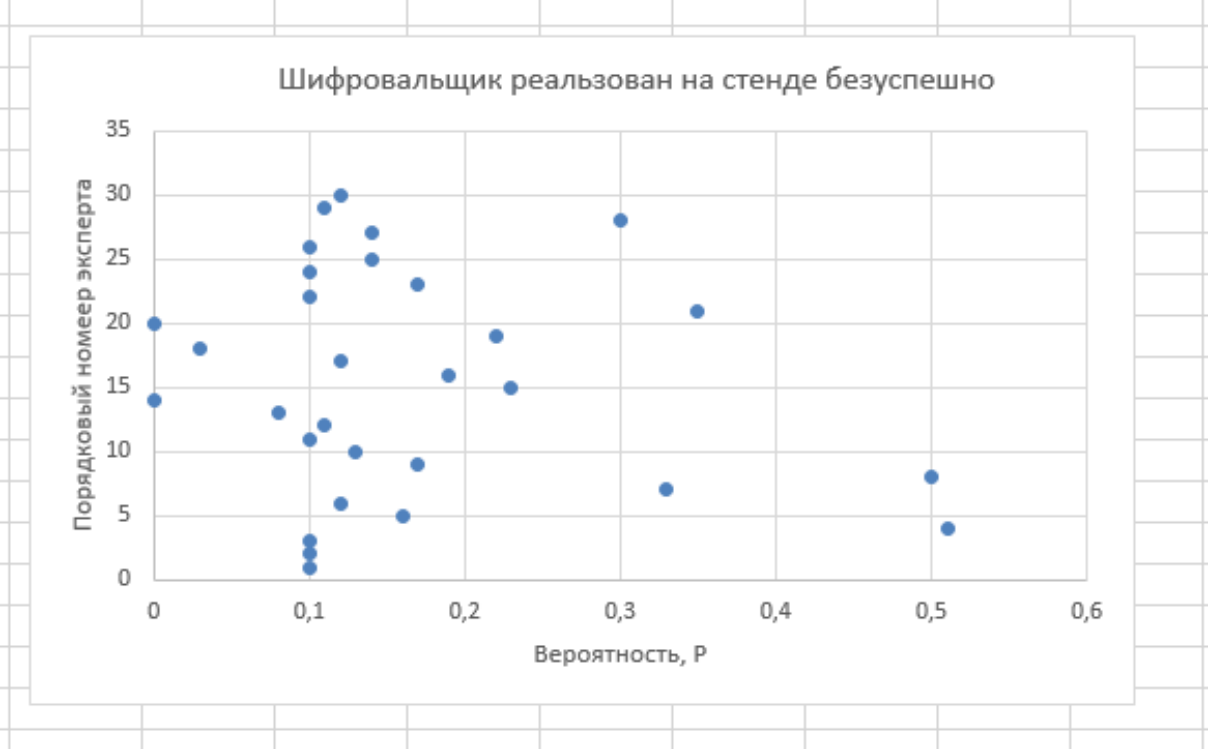

Рис. 28 Точечная диаграмма

Исходя из приведенных результатов, уже можно наблюдать большую разобщенность данных на рисунках 23-34, что свидетельствует о том, что специалисты сильно расхожи в мнениях на задаваемые вопросы. Но в то же время на рисунках 25-28, видно, что данные лежат плотнее друг к другу приближаются к какому-то общему значению, что уже свидетельствует о том, что стен уже помог экспертам приблизиться к какой-то общей оценке. Далее полученные данные были преобразованы в таблицы, для удобства расчета.

Были посчитаны средне арифметические значения для каждого вопроса, результаты получились следующие (1):

$\bar{x}1 = 0{,}211;$

$\bar{x}2 = 0{,}195;$

$\bar{x}3 = 0{,}702;$

$\bar{x}4 = 0{,}668;$

$\bar{x}5 = 0{,}255;$

$\bar{x}6 = 0{,}253;$

Где под каждым номером подразумевается порядковый номер вопроса. Далее были высчитаны среднеквадратичные отклонения, они равняются (2):

$\sigma 1 = 0{,}137;$

$\sigma 2 = 0{,}145;$

$\sigma 3 = 0{,}229;$

$\sigma 4 = 0{,}219;$

$\sigma 5 = 0{,}211;$

$\sigma 6 = 0{,}191;$

После получения значений среднего арифметического и среднеквадратичного отклонения мы задаем уровень доверия. В нашем случае он равняется 95%, так как именно этот уровень позволит оценить, что данные находятся в допустимом для нас пределе.

Затем мы найдем доверительный интервал. Для этого были использованы формулы из 1 главы. Доверительный интервал может показать приблизительный диапазон значений в который будет включена репрезентативная выборка.

Рассчитав доверительный интервал по формуле из первой главы, мы получим следующие значения для каждого вопроса (3):

1 вопрос – без стенда, 0,084;

2 вопрос - без стенда, 0,09;

3 вопрос – со стендом, 0,046;

4 вопрос - со стендом, 0,049;

5 вопрос - со стендом, 0,043;

6 вопрос - со стендом, 0,043;

Границы доверительного интервала для всех значений равны (4):

1 вопрос = 0,084 + 0,293; 0,293 + 0,084;

2 вопрос = 0,09 + 0,281; 0,281 + 0,09;

3 вопрос = 0,046 + 0,790; 0,790 + 0,046;

4 вопрос = 0,049 + 0,774; 0,774 + 0,049;

5 вопрос = 0,043 + 0,174; 0,174 + 0,043;

6 вопрос = 0,043 + 0,164; 0,164 + 0,043;

3.3 Анализ полученных данных

На промежуточных этапах расчет, уже было видно то, как наличие стенда в условии меняет результат вычислений. При просчете среднеквадратичного отклонения оно становилось меньше, чем при расчете тех же данных без стенда. В итоге, беря в расчет 95% уровень доверия, мы можем получить результат в виде разного уровня доверительного интервала до и после стенда.

Исходя из проведенного исследования вероятность реализации угрозы сетевой червь и шифровальщик - вымогатель менялись, в зависимости от поставленных условий, в данном случае наличии или отсутствии стенда и удачной или не удачной реализации атаки на нем. Это говорит о том, что следуя методике, без рассмотрения ее на конкретном примере мы имеем абсолютно разные вероятности реализации угрозы по мнению экспертов.

Как можно увидеть из проделанных расчетов, доверительный интервал оказался ниже именно в том случае, где использовался стенд. Что говорит о точности оценивания измерений, если мы применяем стенд в качестве инструмента повышения достоверности.

Это позволяет говорить о том, что стенд показал себя как решающий параметр в определении вероятности наступления события – реализации или не реализации атаки. А значит он помог повысить достоверность оцениваемой системы, что так же привносит ясность в методику оценивания распределенных информационных систем. Каждая из рассматриваемых информационных систем, перед оцениваем ее экспертом должна быть смоделирована

подходящим для нее образом, так как экспертная оценка не всегда является достоверной в силу тех или иных причин.

Так же в качестве рекомендаций по составленному стенду, могу предложить следующее:

При использовании почтовых систем, которые имеют адрес, расположенный в открытом доступе, следует крайне осторожно относиться к приходящим сообщениям, особенно от незнакомых пользователей. Такой простой и, казалось, бы очевидный совет позволит сократить расходы до 0 в случае возникновения подобного инцидента информационной безопасности, так как не придется привлекать специалистов из профильных организаций для дешифрования данных. Так же стоит обращать внимание на современные системы защиты, затраты на них многократно окупаются, так как система становится еще более защищенной.

Можно с уверенностью сказать, что проделанная работа со стендом себя оправдала, так как мнения экспертов имели наименьший доверительный интервал именно в том случае, когда задавался вопрос с участием стенда и результатов проверки на нем. Это говорит о повышении степени достоверности, в случае практического применения инструментов по моделированию угроз, а также способов защиты от них. Нельзя не сказать так же о том, что отвечая на последние 2 вопроса в анкете, доверительный интервал снизился еще сильнее, что свидетельствует о том, что эксперты приняли его во внимание в вопросах 3-4 и стали доверять его результатам еще больше.

Выводы по данной главе:

В данной главе было произведено исследование, нацеленное на повышение достоверности оценивания распределенной информационной системы экспертом. В качестве метода сбора статистических данных был произведен опрос.

Были собраны данные от 30 специалистов по информационной безопасности разного возраста м разным опытом. Их оценки являлись

объективными в каждом их задаваемых вопросов, поскольку перед ними была четко сформулирована задача исследования. Так же вводных данных о системе было предостаточно для оценки общего уровня защищенности системы и предмет ее устойчивости к угрозам внешнего нарушителя.

Из проведенного анализа можно сказать, что стенд был определяющим фактором в выборе вероятности того или иного события. Так как доверительный интервал уменьшался именно в тех случаях, когда в вопросе фигурировал сам стенд.

ЗАКЛЮЧЕНИЕ

В данной дипломной работе проводился анализ субъекта - Mobileye Corporation на предмет определения того, является ли субъект объектом критической информационной инфраструктуры для дальнейшего обеспечения ее безопасности в рамках требований [1].

Рассмотрен процесс обеспечения функциональности системы. На основе приведенного перечня процессов был сформирован список возможных угроз, и описывались основные методы реализации согласно описанию ФСТЭК БДУ.

Говоря о моделировании реакции распределенной информационной системы, можно сказать что такой подход является многогранным и сложным в некоторых частях своей реализации, но помогает достигнуть поставленного результата, а именно показать на примере стенда работу отдела компании. Сама реализация через фишинговые письма так же показывает, что данный метод остается актуальным в части атаки социальной инженерии. При этом почтовые системы не стоят на месте и не позволяют отправить вирус напрямую, даже если он вшит в картинку или другой файл. Но, несмотря на это, эти же сервисы, что позволяют использовать их облачные хранилища как место для хранения вирусов и не проводят сигнатурный анализ. Это примечательно тем, что вирусы, внедренные в папки с открытым доступом, могут свободно распространяться в интернете. Что может привести к массовому заражению компьютеров, если воспользоваться правильными методами и эффективными средствами социальной инженерии.

Подводя итоги по сделанным расчетам, можно говорить о том, что мнение относительно реализации атаки сетевой-червь и программы-вымогателя, то есть шифровальщика менялась в зависимости от заданных условий, в данном случае наличия стенда для моделирования и удачной или неудачной атаки на него. Из выполненных расчетов видно, что доверительный интервал действительно ниже в случае использования стенда. Это позволяет

говорить о том, что стенд показала себя решающим параметром в определении вероятности события: успеха атаки или ее провала. Таким образом, он помог повысить качество оцениваемой системы.

Для реализации цели исследования были решены следующие задачи:

- Составить описание компании с точки зрения ИБ
- Рассмотрение наиболее распространенных компьютерных вирусов;
- Анализ наиболее актуальных векторов атак;
- Моделирование стенда для реакции РИС;
- Сбор статистических данных от специалистов в сфере информационной безопасности;
- Анализ полученных данных на предмет согласованности при различных условиях.

Считаю выполненными.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Федеральный закон от 26 июля 2017 г. N 187-ФЗ [Электронный ресурс]. Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kii/285-zakony/1610-federalnyj-zakon-ot-26-iyulya-2017-g-n-187-fz (Дата обращения 04.10.2022)
2. Постановление Правительства Российской Федерации от 8 февраля 2018 г. N 127 [Электронный ресурс]. Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kii/287-postanovleniya/1614-postanovlenie-pravitelstva-rossijskoj-federatsii-ot-8-fevralya-2018-g-n-127 (Дата обращения 04.10.2022)
3. Приказ ФСТЭК России от 25 декабря 2017 г. N 239 [Электронный ресурс]. Режим доступа: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (Дата обращения 08.10.2022)
4. Модель нарушителя информационной безопасности [Электронный ресурс]. Режим доступа: https://studopedia.ru/2_37113_model-narushitelya-informatsionnoy-bezopasnosti.html (Дата обращения 17.10.2022)
5. Основные типы компьютерных атак в кредитно-финансовой сфере [Электронный ресурс]. Режим доступа: https://cbr.ru/Collection/Collection/File/32122/Attack_2019-2020.pdf (Дата обращения 15.11.2022)
6. Описание векторов компьютерных атак [Электронный ресурс]. Режим доступа: https://b4.cooksy.ru/articles/opisaniya-vektorov-kompyuternyh-atak-soderzhaschihsya-v-bazah-dannyh (Дата обращения 15.11.2022)
7. Интегратор it информационной безопасности [Электронный ресурс]. Режим доступа:

https://www.dginh.ru/content/umk/it/umk_interprogr_IT_IB_BAS.pdf#2 (Дата обращения 15.11.2022)

8. Информационная безопасность и защита информации: учебно-методическое пособие / Титова Л.Н. 2023. – 76 с.
9. Моделирование компьютерных атак на распределенную информационную систему [Электронный ресурс]. Режим доступа: https://elibrary.ru/item.asp?id=37156211 (Дата обращения 12.01.2023)
10. Что такое Miter ATT&CK и как ее использовать [Электронный ресурс]. Режим доступа: https://blog.tiger-optics.ru/2018/12/what-is-mitre-attack/ (Дата обращения 12.01.2023)
11. Описания векторов компьютерных атак содержащихся в базах данных [Электронный ресурс]. Режим доступа: https://b4.cooksy.ru/articles/opisaniya-vektorov-kompyuternyh-atak-soderzhaschihsya-v-bazah-dannyh
12. На кибербезопасность АСУ ТП направят больше средств [Электронный ресурс]. Режим доступа: https://www.comnews.ru/content/114173/2018-07-30/na-kiberbezopasnost-asu-tp-napravyat-bolshe-sredstv (Дата обращения 17.01.2023)
13. Безопасность организации [Электронный ресурс]. Режим доступа: http://safeorg.ru/archives/527/ (Дата обращения 06.01.2023)
14. Разработка методики прогнозирования динамики изменения вектора компьютерной атаки с точки зрения нарушителя [Электронный ресурс]. Режим доступа: https://elar.urfu.ru/bitstream/10995/106091/1/urfu2338_d.pdf (Дата обращения 18.01.2023)
15. Бурлов В.Г. Математические методы моделирования в экономике. Часть 1. СПб: изд-во СПбГПУ, 2007. - 330 с (Дата обращения 19.01.2023)
16. Выбор наиболее опасных уязвимостей для перспективных информационных систем критического применения [Электронный ресурс]. Режим доступа: https://cyberrus.com/wp-

content/uploads/2022/01/66-75-147-22_7.-Gryzunov.pdf (Дата обращения 19.01.2023)

17. Промышленные компании векторы атак [Электронный ресурс]. Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/ics-attacks-2018/ (Дата обращения 19.01.2023)
18. БДУ ФСТЭК [Электронный ресурс]. Режим доступа: https://bdu.fstec.ru/threat (Дата обращения 29.09.2023)
19. Методический документ. Методика Методика оценки угроз безопасности информации [Электронный ресурс]. Режим доступа: https://fstec.ru/en/component/attachments/download/2919
20. Способы расчета доверительного интервала [Электронный ресурс]. Режим доступа: http://www.estimatica.info/assessment/standards-and-methods/192-sposoby-rascheta-doveritelnogo-intervala (Дата обращения 13.01.2023)
21. Методика оценки угроз безопасности информации [Электронный ресурс]. Режим доступа: https://fstec.ru/component/attachments/download/2919 (Дата обращения 13.01.2023)
22. Положение о Федеральной службе по техническому и экспортному контролю [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_14031/b4771b0410795ff8f613586883b317d567990cc7/ (Дата обращения 06.01.2023)