Подход к определению типовых угроз безопасности информации для промышленных контроллеров

А. А. Асонов[1], А. И. Грюнталь[2], В. Н. Родионов[3]

[1]ФГУ ФНЦ НИИСИ РАН, Москва, Россия, asonow@niisi.ras.ru;

[2]ФГУ ФНЦ НИИСИ РАН, Москва, Россия, grntl@niisi.msk.ru;

[3]ФГУ ФНЦ НИИСИ РАН, Москва, Россия, rodionov@niisi.msk.ru

Аннотация. Определение актуальных угроз безопасности информации для некоторого объекта оценки, как правило, должно проводиться по Методике оценки угроз безопасности, утвержденной 5 февраля 2021 года в качестве методического документа ФСТЭК России. В настоящей статье показано, что при условии, когда к основному элементу объекта оценки, например, к ОС (в составе которого реализуются основные механизмы подсистемы защиты информации от несанкционированного доступа) и для которого существует введенный установленным порядком профиль защиты, перечень типовых угроз безопасности также можно получить из анализа данного документа. Сравнение угроз безопасности информации, полученных из профиля защиты операционных систем типа «В» четвертого класса защиты (ИТ.ОС.В4.ПЗ), с перечнем угроз безопасности информации, полученных из Базы данных ФСТЭК России на основе экспертного метода, после оптимизации данного перечня и исключения из него повторных угроз показывает, что оставшиеся из них находятся в определенном соответствии с угрозами из профиля защиты с некоторой детализацией по их реализации.

Ключевые слова: угроза безопасности информации (УБИ), пользователь УПК, АСУ ТП, операционная система

1. Введение

Под угрозой безопасности информации (УБИ) в соответствии с Методикой оценки угроз безопасности ФСТЭК России [2] понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Определение типовых УБИ, актуальных для промышленного контроллера (ПК), является первым шагом по формированию (уточнению) требований безопасности и в первую очередь функциональных требований безопасности, реализуемых в его составе (на уровне ПК). Установленный перечень типовых УБИ может и должен быть также направлен на обоснование и выбор соответствующих организационных мер защиты информации.

В соответствии с требованиями ФСТЭК России как одного из регуляторов в области защиты информации, в технических заданиях (ТЗ) на разработку конкретных средств обработки информации или в целом автоматизированной системы должны задаваться требования безопасности информации.

При определении источников УБИ и выявлении потенциальных нарушителей и их возможностей по реализации УБИ проводится проверка их взаимосвязи с действующими методическими документами и указаниями ФСТЭК России по данному направлению работ.

В общем виде Методика оценки угроз безопасности [2] существует как методический документ ФСТЭК России, утвержденный 5 февраля 2021 года. Область применения данной методики распространяется на системы и сети, отнесенные к государственным и муниципальным информационным системам (ИС), ИС персональных данных, значимых объектов критической информационной инфраструктуры Российской Федерации, ИС управления производством, используемые организациями оборонно-промышленного комплекса (ОПК), автоматизированные системы управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах и др. (методика введена в действие взамен ранее действующих соответствующих методик ФСТЭК России 2007 и 2008 годов). Особенностью данной методики является то, что в ней УБИ сформулированы и рассматриваются в целом (в общем виде) к системе (например, к АСУ ТП), а определить перечень УБИ типовых (актуальных), собственно, для некоторого элемента системы (в частности ПК) достаточно затруднительно.

В соответствии с Методикой [2] при определении перечня УБИ, типовых для УПК, необходимо также проанализировать перечень УБИ,

содержащийся в банке данных (БД) УБИ ФСТЭК России [6], из которого также должны быть выбраны только те угрозы, которые являются типовыми (актуальными), в частности, для ПК. Необходимо отметить, что в соответствии с Методикой [2] актуальность УБИ также должна определяться наличием и проверкой возможности по реализации сценариев их выполнения.

В целом выявленные актуальные УБИ для ПК могут и должны служить в качестве исходных данных, необходимых для разработки Модели УБИ системы и (или) сети (в частности, АСУ ТП) – требование Методики [2]. При необходимости они могут быть использованы для разработки Частной модели УБИ для ПК.

2. Анализ функциональных требований ПК как составной части АСУ ТП

2.1. Определение основных характеристик ПК, режимов работы и принципов информационного взаимодействия с другими составными частями системы (в частности элементами АСУ ТП)

Анализ базовой функциональной структуры системы с программируемым контроллером, модели аппаратного обеспечения программируемого контроллера, типовой конфигурации интерфейсов / портов ПК-системы, которые приведены в подразделе 4.1 (рис. 1 – 3) ГОСТ Р МЭК 61131-1-2016 [1], показывает следующее.

Аппаратное обеспечение ПК [1] включает: процессорные модули, модули системной шины и питания, модули ввода/вывода, модули передачи данных (необязательное оборудование), терминальные панели модулей ввода вывода, коммуникационные модули и кабели для подключения терминальных панелей к модулям ввода/вывода.

Программное обеспечение ПК [1], как правило, состоит из встраиваемого ПО в составе системного ПО (ОС контроллера, среда исполнения прикладного ПО и др.) и инструментального ПО (набор заголовочных файлов и библиотек ОС, компилятор, удаленный отладчик и др.).

На уровне инструментального ПО реализовываются различные режимы функционирования (режим конфигурирования и настройки ПК, режим наблюдения за работой системного и прикладного ПО, режим отладки, сервисный режим для обслуживания УПК, а также управление механизмами защиты информации (правами доступа пользователей), проверка корректности и целостности алгоритмов прикладного программного обеспечения (ППО), включая сравнение версий проектов и ряд других функций).

Центральной частью ПК является процессорный модуль, который как правило должен находиться под управлением многозадачной высокопроизводительной операционной системы реального времени (ОСРВ). ОСРВ с такими программами, как начальный загрузчик, входные/выходные данные, драйверы коммуникаций, обработчик исключительных ситуаций, планировщик, подсистема диагностики, подсистема управления резервированием и т. д., как правило, входит в состав неизменной части встраиваемого ПО ПК, а к изменяемой части встраиваемого программного обеспечения относится ППО, загружаемое в ПК пользователем.

То, что процессорный модуль (группа модулей) функционирует под управлением ОСРВ, позволяет считать, что основные требования безопасности информации, задаваемые к реализации в ПК, должны разрабатываться именно в составе ОСРВ, а отдельные требования БИ (в случае необходимости) – и на уровне других составных частей ПК.

Большую помощь в проведении данного анализа оказывает наличие технического задания на разработки конкретного ПК.

2.2. Определение потенциальных нарушителей функционирования ПК и их возможностей по реализации УБИ

В качестве непосредственного пользователя ПК, как правило, выступает ее авторизованный оператор или группа операторов, входящих в состав дежурной смены и должностных лиц по обеспечению функционирования, администрирования и обслуживания системы в целом, например, АСУ ТП или ее составной части (отдельного элемента). В целом возможности пользователей ПК (функции оператора и администратора безопасности) определяются возможностями их интерфейсов взаимодействия с ресурсами ОСРВ и средой ее функционирования.

В соответствии с Таблицей 8.1, определяющей уровни возможностей нарушителей по реализации УБИ, приведенной в Методике [3], представитель из данной группы специалистов с точки зрения оценки его возможностей по реализации УБИ потенциально может рассматриваться в качестве нарушителя, обладающего базовыми возможностями или базовыми повышенными возможностями (характеристики **Н1** и **Н2** соответственно). Потенциальные нарушители с характеристиками **Н3**, такие как разработчики программных и программно-аппаратных средств, не рассматриваются в связи с тем, что

после выполнения их работ созданные ими средства проходят все виды испытаний, включая сертификационные, а от выполнения дальнейших работ они как правило отключены. Данный тип нарушителя характеризуется как **внутренний** (относительно средств ПК).

Данные обстоятельства могут накладывать определенные условия и ограничения на выполняемые этими должностными лицами своих функциональных обязанностей по обеспечению функционирования ПК, а также состав УБИ, которые потенциально могут быть реализованы с их стороны. Необходимо также учитывать, что статус администратора безопасности информации ПК в ряде случаев может выводить соответствующее должностное лицо из числа потенциальных нарушителей (может указываться в техническом задании на разработку конкретного ПК, а также определяться из анализа требований безопасности информации по разработке конкретной автоматизированной системы управления технологическими процессами или ее подсистемы).

Установление и согласование с Заказчиком ОКР возможностей нарушителей и их характеристик позволяет разработчику осуществить уточнение состава УБИ, по отношению к которым необходимо проводить мероприятия по защите информации.

2.3 Определение требований безопасности информации, предъявляемых к ПК со стороны системы (например – АСУ ТП)

Анализ требований безопасности информации, предъявляемых в частности к АСУ ТП (для наиболее высокого класса защищенности), в которых применяется ПК, показывает, что такая система должна обеспечивать защищенность до **1 класса защиты** включительно согласно приказу ФСТЭК России от 14 марта 2014 г. № 31 [7], а также в составе значимых объектов критической информационной инфраструктуры до **1 категории значимости** включительно согласно приказу ФСТЭК России от 25 декабря 2017 г. № 239 [8].

Функциональное назначение, принцип обработки информации и место ПК в системе (АСУ ТП) показывает, что уровень конфиденциальности обрабатываемой информации, как правило, характеризует ее как информацию ограниченного доступа («для служебного пользования»), что соответствует требованиям «4 уровню доверия» согласно Приказу ФСТЭК России от 02 июня 2020 г. № 76 [9].

В подразделе 2.1 настоящей статьи сделан вывод, что основным элементом ПК является операционная система (ОСРВ), на уровне которой должны реализовываться основные функции и компоненты безопасности.

Из вышеуказанных требований, вытекает то, что для такого класса защиты АСУ ТП (**1 класс защищенности и 4 уровень доверия**) в соответствии с п. 8 и п. 9 абзаца 4 Приказа ФСТЭК России от 19 августа 2016 г. № 119 [4] им наиболее полно соответствует **ОС 4 класса защиты тип «В»** (ОСРВ).

Рассмотрение и сравнение состава функций безопасности (ФБ), реализуемых с составе ОС типа «В» (ОСРВ) и ОС типа «Б» (встраиваемые ОС), указанных в Таблице 1 Приказа ФСТЭК России от 19 августа 2016 г. № 119, показывает следующее:

- в ОС типа «В» должны быть реализованы все ФБ1 – ФБ8 (ФБ1 – идентификация и аутентификация, ФБ2 – управление доступом, ФБ3 – регистрация событий безопасности, ФБ4 – ограничение программной среды, ФБ5 – изоляция процессов, ФБ6 – защита памяти, ФБ7 – контроль целостности компонентов ОС, а также иных объектов файловой системы, ФБ8 – обеспечение надежного функционирования);
- в ОС типа «Б» из ФБ1 – ФБ8 отсутствуют требования по реализации ФБ5 и ФБ7.

Частный вывод: ОС типа «В» по сравнению с ОС типа «Б» в части предъявляемых и реализуемых ФБ является более функционально полной.

3. Определение перечня типовых (актуальных) угроз безопасности информации ПК

Однозначное представление о типовых (актуальных) УБИ, которым должна противостоять ОСРВ, дает профиль защиты [5], в нашем случае Методический документ ФСТЭК России «Профиль защиты (ПЗ) операционных систем типа «В» четвертого класса защиты» – ИТ.ОС.В4.ПЗ [4]. Среди угроз, которым должна противостоять ОСРВ, угрозы У1 – У11 и угрозы, которым должна противостоять среда функционирования ОСРВ, УС1 – УС7 (обозначение угроз дано в соответствии с ПЗ).

С другой стороны, возникает необходимость проверить, как угрозы из профиля защиты соотносятся с угрозами БИ, приведенными в базе данных угроз (БД) ФСТЭК России.

Все УБИ, представленные в БД угроз (222 угрозы), были рассмотрены и из них были выбраны только те, которые могут оказывать влияние на функционирование ПК (отбор проводился в соответствии с характеристиками, указанными в БД: **«объект воздействия»** – это ПК (один из элементов АСУ ТП); **«источник угрозы»** – это внутренний нарушитель – ВН с

низким потенциалом – **Н1** и средним потенциалом – **Н2** (из-за принятого в подразделе 2.2 соглашения внутренний нарушитель с высоким потенциалом – **Н3** не рассматривается). Проведение выбора из приведенных угроз в БД осуществлялось на основе экспертного метода специалистами разработчика. При необходимости дополнительная минимизация УБИ может проводиться по характеристике БД **«последствия реализации угрозы»** (нарушение конфиденциальности, целостности, доступности – выбору подлежат только те УБИ из БД, для которых эта характеристика задана или является существенной).

Все данные по выбору УБИ из ПЗ и их сопоставлению с УБИ из БД ФСТЭК России отображены в Таблице 1 (см. Приложение к статье).

В Таблице 1 представлены УБИ, выбранные из ПЗ, в сопоставлении с УБИ, выбранными из Базы данных УБИ ФСТЭК России [6] (второй столбец таблицы). В третьем столбце Таблицы 1 за каждой УБИ из ПЗ отражены УБИ из базы как наиболее типовые (актуальные) для ПК. Порядок выбора был следующим: из общего числа выбранных угроз из базы, если они повторялись по отношению к У1 – У11 и УС1 – УС7, в третьем столбце таблицы отражается только одна угроза (например, УБИ.015 (отмечена экспертом) соответствует У1 и УС2, но в последующем для У1 она была убрана (исключена из рассмотрения в связи с повтором), а для УС2 оставлена как наиболее характерная для этого случая). Данный подход выполнялся для всех УБИ из базы.

Предполагается, что выполнение данного анализа позволит более детально рассмотреть угрозы БИ из БД с точки зрения их устранения при реализации конкретной архитектуры ПК (ее составных частей) с учетом условий эксплуатации создаваемого изделия, отмеченных в эксплуатационной документации в рамках установленных испытаний образца и в ходе его сертификационных испытаний (например, устранение «УБИ.165: Угроза включения в проект не достоверно испытанных компонентов», как правило, проверяется в рамках приемочных испытаний опытного образца изделия).

При этом необходимо учитывать, что отдельные угрозы парируются организационными или организационно-техническими мерами (например, У5, (УБИ012) – конкретной регламентацией (до отдельного параметра) за конфигурированием ПО (ОС) и организацией контроля за выполнением данных работ и др.).

При определении типовых (актуальных) угроз БИ, необходимо учитывать такой факт, что в ПК, как правило, одновременно могут существовать не более двух пользователей (см. замечание выше), функциональные обязанности которых предполагают все аспекты деятельности практически со всеми его ресурсами.

Анализ угроз из БД ФСТЭК России показывает, что определенная их часть также должна дополнительно рассматриваться и решаться интегратором при создании конкретного АСУ ТП (при встраивании ПК в систему в качестве ее составной части), в частности при разработке частных руководств и инструкций по его применению.

При проведении данной работы в практическом плане необходимо учитывать и то, что часть УБИ сформированы таким образом, что они должны «парироваться» исключительно организационными мерами.

Выполнение минимизации перечня УБИ позволит сократить его не менее чем в два-три раза и упростит их дальнейшее рассмотрение.

4. Заключение

Приведенное в Таблице 1 сравнение угроз безопасности информации, полученных из ПЗ, с перечнем угроз безопасности информации, полученных из БД ФСТЭК России на основе экспертного метода, после оптимизации данного перечня и исключения из него повторных угроз показывает, что оставшиеся из них находятся в очевидном соответствии с угрозами из профиля защиты с некоторой детализацией по их реализации.

В целом предложенный подход по определению УБИ, типовых для конкретного элемента автоматизированной системы (в частности ПК), базирующийся на наличии и использовании исходных данных заказчика, а также наличие НМД (нормативно-методической документации) Регулятора в области защиты (в статье это профиль защиты для ОС типа «В» 4 класса защиты и УБИ БД ФСТЭК России) позволяет значительно сократить время для выполнения этой работы.

С точки зрения эффективности данный подход позволяет получить результаты аналогичные, но не хуже по сравнению с методом, приведенным в Методическом документе ФСТЭК России «Методика оценки угроз безопасности информации», утвержденном ФСТЭК России 5 февраля 2021 года (подход и метод базируются на проведении экспертных оценок).

Публикация выполнена в рамках государственного задания по проведению фундаментальных исследований по теме «Исследование и реализация программной платформы для перспективных многоядерных процессоров» (FNEF-2022-002).

ПРИЛОЖЕНИЕ

Таблица 1. Соответствие УБИ из ПЗ угрозам безопасности из Базы данных УБИ ФСТЭК России

УБИ из ПЗ (указатель и аннотация), характеристика нарушителя (ВН – внутренний, ВНЕШ – внешний)	**УБИ из БД ФСТЭК России (указатель и аннотация)**	**УБИ из БД ФСТЭК России (указатель и аннотация) с учетом исключения повторных УБИ**
У1 – НСД к объектам доступа со стороны субъектов доступа, для которых запрашиваемый доступ не разрешен (ВН)	УБИ.015: Угроза доступа к защищаемым файлам с использованием обходного пути УБИ.028: Угроза использования альтернативных путей доступа к ресурсам УБИ.033: Угроза использования слабостей кодирования входных данных УБИ.034: Угроза использования слабостей протоколов сетевого/локального обмена данными УБИ.036: Угроза исследования механизмов работы программы УБИ.037: Угроза исследования приложения через отчеты об ошибках УБИ.067: Угроза неправомерного ознакомления с защищаемой информацией УБИ.068: Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением УБИ.073: Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети УБИ.074: Угроза несанкционированного доступа к аутентификационной информации УБИ.075: Угроза несанкционированного доступа к виртуальным каналам передачи УБИ.076: Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети УБИ.077: Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение УБИ.080: Угроза несанкционированного доступа к защищаемым	УБИ.033: Угроза использования слабостей кодирования входных данных УБИ.067: Угроза неправомерного ознакомления с защищаемой информацией УБИ.073: Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети УБИ.075: Угроза несанкционированного доступа к виртуальным каналам передачи УБИ.076: Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети УБИ.077: Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение УБИ.080: Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети УБИ.083: Угроза несанкционированного доступа к системе по беспроводным каналам УБИ.084: Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети УБИ.085: Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации УБИ.090: Угроза несанкционированного создания учетной записи пользователя УБИ.092: Угроза несанкционированного удаленного внеполосного доступа к аппаратным средствам УБИ.207: Угроза несанкционированного доступа к параметрам

	виртуальным устройствам из виртуальной и (или) физической сети УБИ.083: Угроза несанкционированного доступа к системе по беспроводным каналам УБИ.084: Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети УБИ.085: Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации УБИ.090: Угроза несанкционированного создания учетной записи пользователя УБИ.092: Угроза несанкционированного удаленного внеполосного доступа к аппаратным средствам УБИ.116: Угроза перехвата данных, передаваемых по вычислительной сети УБИ.127: Угроза подмены действия пользователя путем обмана УБИ.128: Угроза подмены доверенного пользователя УБИ.131: Угроза подмены субъекта сетевого доступа УБИ.160: Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.165: Угроза включения в проект не достоверно испытанных компонентов УБИ.187: Угроза несанкционированного воздействия на средство защиты информации УБИ.189: Угроза маскирования действий вредоносного кода УБИ.195: Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы УБИ.207: Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей) УБИ.209: Угроза несанкционированного доступа к защищаемой памяти ядра процессора УБИ.214: Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	настройки оборудования за счет использования «мастер-кодов» (инженерных паролей) УБИ.209: Угроза несанкционированного доступа к защищаемой памяти ядра процессора

	УБИ.215: Угроза несанкционированного доступа к системе при помощи сторонних сервисов	
У2 – ограничение нарушителем доступа пользователей ОС к ресурсам СВТ, на котором установлена ОС за счет длительного удержания вычислительного ресурса в загруженном состоянии путем осуществления нарушителем многократных запросов, требующих большого количества ресурсов на их обработку (ВН)	УБИ.014: угроза длительного удержания вычислительных ресурсов пользователями (ВН, ВНЕШ). Объекты доступа – сетевой трафик, сетевое ПО, сетевой узел, системное ПО УБИ.028: Угроза использования альтернативных путей доступа к ресурсам УБИ.034: Угроза использования слабостей протоколов сетевого/локального обмена данными УБИ.059: Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов УБИ.068: Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением УБИ.069: Угроза неправомерных действий в каналах связи УБИ.098: Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб УБИ.128: Угроза подмены доверенного пользователя УБИ.140: Угроза приведения системы в состояние «отказ в обслуживании» УБИ.153: Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов УБИ.155: Угроза утраты вычислительных ресурсов УБИ.165: Угроза включения в проект не достоверно испытанных компонентов УБИ.169: Угроза наличия механизмов разработчика УБИ.176: Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты УБИ.183: Угроза перехвата управления автоматизированной системой управления технологическими процессами УБИ.187: Угроза несанкционированного воздействия на средство защиты информации УБИ.189: Угроза маскирования действий вредоносного кода УБИ.192: Угроза использования уяз-	УБИ.028: Угроза использования альтернативных путей доступа к ресурсам УБИ.034: Угроза использования слабостей протоколов сетевого/локального обмена данными УБИ.098: Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб УБИ.153: Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов

	вимых версий программного обеспечения УБИ.195: Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы УБИ.208: Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники УБИ.214: Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	
У3 – несанкционированное или ошибочное удаление информации с СВТ, функционирующего под управлением ОС (ВН)	УБИ.034: Угроза использования слабостей протоколов сетевого/локального обмена данными УБИ.036: Угроза исследования механизмов работы программы УБИ.068: Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением УБИ.069: Угроза неправомерных действий в каналах связи УБИ.091: Угроза несанкционированного удаления защищаемой информации УБИ.127: Угроза подмены действия пользователя путем обмана УБИ.128: Угроза подмены доверенного пользователя УБИ.143: Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.152: Угроза удаления аутентификационной информации УБИ.156: Угроза утраты носителей информации УБИ.157: Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.158: Угроза форматирования носителей информации УБИ.160: Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.165: Угроза включения в проект не достоверно испытанных компонентов УБИ.169: Угроза наличия механизмов разработчика УБИ.182: Угроза физического устаревания аппаратных компонентов	УБИ.091: Угроза несанкционированного удаления защищаемой информации УБИ.143: Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.152: Угроза удаления аутентификационной информации УБИ.158: Угроза форматирования носителей информации

	УБИ.183: Угроза перехвата управления автоматизированной системой управления технологическими процессами УБИ.187: Угроза несанкционированного воздействия на средство защиты информации УБИ.189: Угроза маскирования действий вредоносного кода УБИ.192: Угроза использования уязвимых версий программного обеспечения УБИ.195: Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы УБИ.214: Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	
У4 – утечка или несанкционированное изменение информации в ОП, используемой различными процессами и формируемыми ими потоками (ВН и ВНЕШ)	УБИ.025: Угроза изменения системных и глобальных переменных УБИ.026: Угроза искажения XML-схемы УБИ.036: Угроза исследования механизмов работы программы УБИ.037: Угроза исследования приложения через отчеты об ошибках УБИ.069: Угроза неправомерных действий в каналах связи УБИ.086: Угроза несанкционированного изменения аутентификационной информации УБИ.116: Угроза перехвата данных, передаваемых по вычислительной сети УБИ.128: Угроза подмены доверенного пользователя УБИ.132: Угроза получения предварительной информации об объекте защиты УБИ.160: Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.165: Угроза включения в проект не достоверно испытанных компонентов УБИ.169: Угроза наличия механизмов разработчика УБИ.183: Угроза перехвата управления автоматизированной системой управления технологическими процессами УБИ.185: Угроза несанкционированного изменения параметров	УБИ.025: Угроза изменения системных и глобальных переменных УБИ.132: Угроза получения предварительной информации об объекте защиты УБИ.169: Угроза наличия механизмов разработчика УБИ.189: Угроза маскирования действий вредоносного кода УБИ.192: Угроза использования уязвимых версий программного обеспечения УБИ.193: Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика УБИ.203: Угроза утечки информации с неподключенных к сети Интернет компьютеров

	настройки средств защиты информации УБИ.187: Угроза несанкционированного воздействия на средство защиты информации УБИ.189: Угроза маскирования действий вредоносного кода УБИ.192: Угроза использования уязвимых версий программного обеспечения УБИ.193: Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика УБИ.195: Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы УБИ.203: Угроза утечки информации с неподключенных к сети Интернет компьютеров УБИ.214: Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	
У5 – несанкционированное внесение нарушителем изменений в конфигурационные (и иные) данные, которые влияют на функционирование отдельных сервисов, приложений или ОС в целом (ВН)	УБИ.012 – угроза деструктивного изменения конфигурации/среды окружения ПО Объекты доступа – системное ПО, ППО, сетевое ПО, микропрограммное обеспечение УБИ.023: Угроза изменения компонентов информационной (автоматизированной) системы УБИ.025: Угроза изменения системных и глобальных переменных УБИ.026: Угроза искажения XML-схемы УБИ.036: Угроза исследования механизмов работы программы УБИ.037: Угроза исследования приложения через отчеты об ошибках УБИ.068: Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением УБИ.127: Угроза подмены действия пользователя путем обмана УБИ.128: Угроза подмены доверенного пользователя УБИ.160: Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.169: Угроза наличия механизмов разработчика	УБИ.012 – угроза деструктивного изменения конфигурации/среды окружения ПО Объекты доступа – системное ПО, ППО, сетевое ПО, микропрограммное обеспечение УБИ.023: Угроза изменения компонентов информационной (автоматизированной) системы УБИ.026: Угроза искажения XML-схемы УБИ.183: Угроза перехвата управления автоматизированной системой управления технологическими процессами УБИ.185: Угроза несанкционированного изменения параметров настройки средств защиты информации УБИ.195: Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы УБИ.204: Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров

	УБИ.179: Угроза несанкционированной модификации защищаемой информации УБИ.183: Угроза перехвата управления автоматизированной системой управления технологическими процессами УБИ.185: Угроза несанкционированного изменения параметров настройки средств защиты информации УБИ.187: Угроза несанкционированного воздействия на средство защиты информации УБИ.189: Угроза маскирования действий вредоносного кода УБИ.192: Угроза использования уязвимых версий программного обеспечения УБИ.195: Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы УБИ.204: Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров УБИ.214: Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	
У6 – осуществление восстановления (подбора) аутентификационной информации пользователей ОС (ВН и ВНЕШ)	УБИ.008: Угроза восстановления и/или повторного использования аутентификационной информации УБИ.030: Угроза использования информации идентификации/аутентификации, заданной по умолчанию УБИ.034: Угроза использования слабостей протоколов сетевого/локального обмена данными УБИ.036: Угроза исследования механизмов работы программы УБИ.067: Угроза неправомерного ознакомления с защищаемой информацией УБИ.074: Угроза несанкционированного доступа к аутентификационной информации УБИ.100: Угроза обхода некорректно настроенных механизмов аутентификации УБИ.160: Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	УБИ.008: Угроза восстановления и/или повторного использования аутентификационной информации УБИ.213: Угроза обхода многофакторной аутентификации

	УБИ.169: Угроза наличия механизмов разработчика УБИ.192: Угроза использования уязвимых версий программного обеспечения УБИ.195: Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы УБИ.213: Угроза обхода многофакторной аутентификации УБИ.214: Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	
У7 – использование нарушителем идентификационной и начальной аутентификационной информации, соответствующей учетной записи пользователя ОС (ВН и ВНЕШ)	УБИ.030 – угроза использования информации идентификации/аутентификации заданной по умолчанию УБИ.067: Угроза неправомерного ознакомления с защищаемой информацией УБИ.127: Угроза подмены действия пользователя путем обмана УБИ.128: Угроза подмены доверенного пользователя УБИ.165: Угроза включения в проект не достоверно испытанных компонентов УБИ.169: Угроза наличия механизмов разработчика УБИ.192: Угроза использования уязвимых версий программного обеспечения УБИ.195: Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы УБИ.214: Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	УБИ.030 – угроза использования информации идентификации/аутентификации заданной по умолчанию УБИ.127: Угроза подмены действия пользователя путем обмана УБИ.128: Угроза подмены доверенного пользователя
У8 – несанкционированное внесение изменений в журналы регистрации событий безопасности ОС (ВН)	УБИ.037: Угроза исследования приложения через отчеты об ошибках УБИ.068: Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением УБИ.124: Угроза подделки записей журнала регистрации событий УБИ.127: Угроза подмены действия пользователя путем обмана УБИ.128: Угроза подмены доверенного пользователя УБИ.160: Угроза хищения средств	УБИ.037: Угроза исследования приложения через отчеты об ошибках УБИ.179: Угроза несанкционированной модификации защищаемой информации

	хранения, обработки и (или) ввода/вывода/передачи информации УБИ.165: Угроза включения в проект не достоверно испытанных компонентов УБИ.169: Угроза наличия механизмов разработчика УБИ.179: Угроза несанкционированной модификации защищаемой информации УБИ.183: Угроза перехвата управления автоматизированной системой управления технологическими процессами УБИ.187: Угроза несанкционированного воздействия на средство защиты информации УБИ.189: Угроза маскирования действий вредоносного кода УБИ.192: Угроза использования уязвимых версий программного обеспечения УБИ.195: Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы УБИ.214: Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	
У9 – НСД к информации вследствие использования пользователями ОС неразрешенного ПО (ВН)	УБИ.067: Угроза неправомерного ознакомления с защищаемой информацией УБИ.068: Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением УБИ.116: Угроза перехвата данных, передаваемых по вычислительной сети УБИ.132: Угроза получения предварительной информации об объекте защиты УБИ.160: Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.165: Угроза включения в проект не достоверно испытанных компонентов УБИ.183: Угроза перехвата управления автоматизированной системой управления технологическими процессами УБИ.187: Угроза несанкционированного воздействия на средство защиты информации	УБИ.188: Угроза подмены программного обеспечения УБИ.191: Угроза внедрения вредоносного кода в дистрибутив программного обеспечения УБИ.211: Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем УБИ.217: Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения

	УБИ.188: Угроза подмены программного обеспечения УБИ.189: Угроза маскирования действий вредоносного кода УБИ.191: Угроза внедрения вредоносного кода в дистрибутив программного обеспечения УБИ.192: Угроза использования уязвимых версий программного обеспечения УБИ.195: Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы УБИ.211: Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем УБИ.217: Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения УБИ.214: Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	
У10 – НСБ субъектов доступа к информации, обработка которой осуществлялась в рамках сеансов (сессий) других субъектов доступа (ВН)	УБИ.034: Угроза использования слабостей протоколов сетевого/локального обмена данными УБИ.067: Угроза неправомерного ознакомления с защищаемой информацией УБИ.074: Угроза несанкционированного доступа к аутентификационной информации УБИ.116: Угроза перехвата данных, передаваемых по вычислительной сети УБИ.127: Угроза подмены действия пользователя путем обмана УБИ.128: Угроза подмены доверенного пользователя УБИ.131: Угроза подмены субъекта сетевого доступа УБИ.160: Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.165: Угроза включения в проект не достоверно испытанных компонентов УБИ.192: Угроза использования уязвимых версий программного обеспечения	УБИ.116: Угроза перехвата данных, передаваемых по вычислительной сети УБИ.131: Угроза подмены субъекта сетевого доступа УБИ.215: Угроза несанкционированного доступа к системе при помощи сторонних сервисов

	УБИ.195: Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы УБИ.215: Угроза несанкционированного доступа к системе при помощи сторонних сервисов	
У11 – недоступность вычислительных ресурсов (процессорное время, ОП и др.) для критических служб ОС и функционирующего ППО (приложений) вследствие нерационального распределения ресурсов между потоками служб и приложений (без учета степени критичности) (ВН)	УБИ.014: Угроза длительного удержания вычислительных ресурсов пользователями УБИ.022 – угроза избыточного выделения ОП УБИ.038: Угроза исчерпания вычислительных ресурсов хранилища больших данных УБИ.059: Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов УБИ.069: Угроза неправомерных действий в каналах связи УБИ.098: Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб УБИ.128: Угроза подмены доверенного пользователя УБИ.140: Угроза приведения системы в состояние «отказ в обслуживании» УБИ.155: Угроза утраты вычислительных ресурсов УБИ.160: Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.165: Угроза включения в проект не достоверно испытанных компонентов УБИ.166: Угроза внедрения системной избыточности УБИ.169: Угроза наличия механизмов разработчика УБИ.176: Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты УБИ.179: Угроза несанкционированной модификации защищаемой информации УБИ.182: Угроза физического устаревания аппаратных компонентов УБИ.183: Угроза перехвата управления автоматизированной системой управления технологическими процессами УБИ.187: Угроза несанкционированного воздействия на средство защиты информации УБИ.189: Угроза маскирования действий вредоносного кода	УБИ.014: Угроза длительного удержания вычислительных ресурсов пользователями УБИ.022 – угроза избыточного выделения ОП УБИ.038: Угроза исчерпания вычислительных ресурсов хранилища больших данных УБИ.059: Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов УБИ.140: Угроза приведения системы в состояние «отказ в обслуживании» УБИ.155: Угроза утраты вычислительных ресурсов УБИ.208: Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники

	УБИ.192: Угроза использования уязвимых версий программного обеспечения УБИ.195: Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы УБИ.208: Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники УБИ.214: Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	
УС1 – нарушение целостности программных компонентов ОС (ВН и ВНЕШ)	УБИ.026: Угроза искажения XML-схемы УБИ.036: Угроза исследования механизмов работы программы УБИ.037: Угроза исследования приложения через отчеты об ошибках УБИ.068: Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением УБИ.069: Угроза неправомерных действий в каналах связи УБИ.143: Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.156: Угроза утраты носителей информации УБИ.157: Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.160: Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.165: Угроза включения в проект не достоверно испытанных компонентов УБИ.169: Угроза наличия механизмов разработчика УБИ.179: Угроза несанкционированной модификации защищаемой информации УБИ.182: Угроза физического устаревания аппаратных компонентов УБИ.183: Угроза перехвата управления автоматизированной системой управления технологическими процессами УБИ.187: Угроза несанкциониро-	УБИ.036: Угроза исследования механизмов работы программы УБИ.068: Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением УБИ.069: Угроза неправомерных действий в каналах связи УБИ.156: Угроза утраты носителей информации УБИ.165: Угроза включения в проект не достоверно испытанных компонентов

	ванного воздействия на средство защиты информации УБИ.189: Угроза маскирования действий вредоносного кода УБИ.192: Угроза использования уязвимых версий программного обеспечения УБИ.195: Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы УБИ.214: Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	
УС2 – отключение и (или) обход нарушителями компонентов ОС, реализующих функции БИ путем подмены нарушителями загружаемой ОС (ВН и ВНЕШ)	УБИ.015 – угроза доступа к защищенным файлам с использованием обходного пути УБИ.018 – угроза связанная с подменой ОС при загрузке путем несанкционированного переконфигурирования BIOS|UEF1 пути доступа к загрузчику ОС УБИ.034: Угроза использования слабостей протоколов сетевого/локального обмена данными УБИ.036: Угроза исследования механизмов работы программы УБИ.068: Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением УБИ.127: Угроза подмены действия пользователя путем обмана УБИ.128: Угроза подмены доверенного пользователя УБИ.160: Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.179: Угроза несанкционированной модификации защищаемой информации УБИ.183: Угроза перехвата управления автоматизированной системой управления технологическими процессами УБИ.187: Угроза несанкционированного воздействия на средство защиты информации УБИ.189: Угроза маскирования действий вредоносного кода УБИ.192: Угроза использования уязвимых версий программного обеспечения УБИ.195: Угроза удаленного за-	УБИ.015 – угроза доступа к защищенным файлам с использованием обходного пути УБИ.018 – угроза связанная с подменой ОС при загрузке путем несанкционированного переконфигурирования BIOS|UEF1 пути доступа к загрузчику ОС УБИ.214: Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации

	пуска вредоносного кода в обход механизмов защиты операционной системы УБИ.214: Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	
УС3 – нарушение целостности данных (в т. ч. параметров настройки СЗИ ОС (ВН и ВНЕШ)	УБИ.049: Угроза нарушения целостности данных кеша УБИ.068: Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением УБИ.143: Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.145: Угроза пропуска проверки целостности программного обеспечения УБИ.156: Угроза утраты носителей информации УБИ.157: Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.160: Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.165: Угроза включения в проект не достоверно испытанных компонентов УБИ.169: Угроза наличия механизмов разработчика УБИ.179: Угроза несанкционированной модификации защищаемой информации УБИ.182: Угроза физического устаревания аппаратных компонентов УБИ.183: Угроза перехвата управления автоматизированной системой управления технологическими процессами УБИ.187: Угроза несанкционированного воздействия на средство защиты информации УБИ.189: Угроза маскирования действий вредоносного кода УБИ.192: Угроза использования уязвимых версий программного обеспечения УБИ.195: Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы УБИ.214: Угроза несвоевременного	УБИ.049: Угроза нарушения целостности данных кеша УБИ.145: Угроза пропуска проверки целостности программного обеспечения УБИ.157: Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.187: Угроза несанкционированного воздействия на средство защиты информации

	выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	
УС4 – НСД нарушителя к аутентификационной информации администраторов и (или) пользователей ОС (ВН и ВНЕШ)	УБИ.008: Угроза восстановления и/или повторного использования аутентификационной информации УБИ.030: Угроза использования информации идентификации/аутентификации, заданной по умолчанию УБИ.036: Угроза исследования механизмов работы программы УБИ.067: Угроза неправомерного ознакомления с защищаемой информацией УБИ.074: Угроза несанкционированного доступа к аутентификационной информации УБИ.086: Угроза несанкционированного изменения аутентификационной информации УБИ.090: Угроза несанкционированного создания учетной записи пользователя УБИ.100: Угроза обхода некорректно настроенных механизмов аутентификации УБИ.116: Угроза перехвата данных, передаваемых по вычислительной сети УБИ.127: Угроза подмены действия пользователя путем обмана УБИ.128: Угроза подмены доверенного пользователя УБИ.160: Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.165: Угроза включения в проект не достоверно испытанных компонентов УБИ.187: Угроза несанкционированного воздействия на средство защиты информации УБИ.189: Угроза маскирования действий вредоносного кода УБИ.192: Угроза использования уязвимых версий программного обеспечения УБИ.195: Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы УБИ.198: Угроза скрытной регистрации вредоносной программой учетных записей администраторов УБИ.214: Угроза несвоевременного	УБИ.074: Угроза несанкционированного доступа к аутентификационной информации УБИ.086: Угроза несанкционированного изменения аутентификационной информации УБИ.100: Угроза обхода некорректно настроенных механизмов аутентификации УБИ.198: Угроза скрытной регистрации вредоносной программой учетных записей администраторов

	выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	
УС5 – несанкционированное внесение нарушителем изменений в журналы регистрации событий безопасности ОС за счет доступа к файлам журналов регистрации событий безопасности ОС в среде функционирования ОС с использованием специальных программных средств, предоставляющих возможность обрабатывать файлы журналов регистрации событий безопасности ОС (ВН)	УБИ.037: Угроза исследования приложения через отчеты об ошибках УБИ.068: Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением УБИ.124: Угроза подделки записей журнала регистрации событий УБИ.127: Угроза подмены действия пользователя путем обмана УБИ.128: Угроза подмены доверенного пользователя УБИ.169: Угроза наличия механизмов разработчика УБИ.179: Угроза несанкционированной модификации защищаемой информации УБИ.183: Угроза перехвата управления автоматизированной системой управления технологическими процессами УБИ.187: Угроза несанкционированного воздействия на средство защиты информации УБИ.189: Угроза маскирования действий вредоносного кода УБИ.192: Угроза использования уязвимых версий программного обеспечения УБИ.195: Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы УБИ.214: Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	УБИ.124: Угроза подделки записей журнала регистрации событий
УС6 – несанкционированное копирование информации из памяти СВТ на съемные МНИ (или другое место вне информационной системы) пользователем ОС (ВН)	УБИ.034: Угроза использования слабостей протоколов сетевого/локального обмена данными УБИ.057: Угроза неконтролируемого копирования данных внутри хранилища больших данных УБИ.067: Угроза неправомерного ознакомления с защищаемой информацией УБИ.068: Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением УБИ.069: Угроза неправомерных	УБИ.057: Угроза неконтролируемого копирования данных внутри хранилища больших данных УБИ.088: Угроза несанкционированного копирования защищаемой информации УБИ.160: Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации

	действий в каналах связи УБИ.088: Угроза несанкционированного копирования защищаемой информации УБИ.116: Угроза перехвата данных, передаваемых по вычислительной сети УБИ.127: Угроза подмены действия пользователя путем обмана УБИ.128: Угроза подмены доверенного пользователя УБИ.132: Угроза получения предварительной информации об объекте защиты УБИ.160: Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.165: Угроза включения в проект не достоверно испытанных компонентов УБИ.169: Угроза наличия механизмов разработчика УБИ.183: Угроза перехвата управления автоматизированной системой управления технологическими процессами УБИ.187: Угроза несанкционированного воздействия на средство защиты информации УБИ.189: Угроза маскирования действий вредоносного кода УБИ.192: Угроза использования уязвимых версий программного обеспечения УБИ.195: Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы УБИ.214: Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	
УС7 – снижение производительности ОС из-за внедрения в нее избыточного ПО и его компонентов (ВН)	УБИ.022: Угроза избыточного выделения оперативной памяти УБИ.036: Угроза исследования механизмов работы программы УБИ.059: Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов УБИ.068: Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением УБИ.127: Угроза подмены действия пользователя путем обмана	УБИ.161: Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями УБИ.166: Угроза внедрения системной избыточности УБИ.176: Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты УБИ.180: Угроза отказа подсистемы обеспечения температурного режима

	УБИ.155: Угроза утраты вычислительных ресурсов УБИ.160: Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.161: Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями УБИ.165: Угроза включения в проект не достоверно испытанных компонентов УБИ.166: Угроза внедрения системной избыточности УБИ.169: Угроза наличия механизмов разработчика УБИ.176: Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты УБИ.179: Угроза несанкционированной модификации защищаемой информации УБИ.180: Угроза отказа подсистемы обеспечения температурного режима УБИ.182: Угроза физического устаревания аппаратных компонентов УБИ.183: Угроза перехвата управления автоматизированной системой управления технологическими процессами УБИ.187: Угроза несанкционированного воздействия на средство защиты информации УБИ.189: Угроза маскирования действий вредоносного кода УБИ.192: Угроза использования уязвимых версий программного обеспечения УБИ.195: Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы УБИ.208: Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники УБИ.214: Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	УБИ.182: Угроза физического устаревания аппаратных компонентов

An Approach to Identifying Information Security Threats Relevant and Specific for a Universal Industrial Controller

Alexander Asonov, Andrey Gruntal, Victor Rodionov

Abstract. Determining current threats to information security for a certain object of assessment, as a rule, should be carried out according to the Methodology for Assessing Security Threats, approved on February 5, 2021 as a methodological document of the FSTEC of Russia. This article shows that, provided that the main element of the assessment object, e.g., OS, (which implements the main mechanisms of the subsystem for protecting information from unauthorized access) and for which there is a security profile introduced in the established order, the list of typical security threats can also be obtained from the analysis of this document. Comparison of information security threats obtained from the security profile of operating systems of type "B" of the 4th security class, with a list of information security threats obtained from the FSTEC of Russia Database based on the expert method, after optimizing this list and the exclusion of repeated threats from it, shows that the remaining threats are in certain correspondence with the threats from the security profile with some detail on their implementation.

Keywords: information security threat, universal industrial controller, automated process control system, operating system

Литература

1. Контроллеры программируемые. Часть 1. Общая информация (IEC 61131-1:2003, IDT). URL: https://docs.cntd.ru/document/1200135007 (дата обращения 13.10.2023).

2. «Методика оценки угроз безопасности информации». Методический документ ФСТЭК России, утвержден 5 февраля 2021 года. URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (дата обращения 13.10.2023).

3. Приказ ФСТЭК России от 9 августа 2018 г. № 138 «О внесении изменений в требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и окружающей природной среды, утвержденные приказом ФСТЭК России от 14 марта 2014 г. № 31, и в требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденными приказом ФСТЭК России от 25 декабря 2017 г. № 239».

4. Приказ ФСТЭК России от 19 августа 2016 г. № 119 «Требования в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации ограниченного доступа (требования безопасности информации к операционным системам)».

5. Методический документ. «Профиль защиты операционных систем типа «В» четвертого класса защиты – ИТ.ОС.В4.ПЗ». https://www.garant.ru/products/ipo/prime/doc/71588736/ (дата обращения 13.10.2023).

6. «Банк данных угроз безопасности информации ФСТЭК России». URL: https://bdu.fstec.ru (дата обращения 13.10.2023).

7. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды». URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (дата обращения 13.10.2023).

8. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры российской федерации». URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (дата обращения 13.10.2023).

9. Приказ ФСТЭК России № 76 от 02.06.2020 «Об утверждении Требований по безопасности информации, устанавливающих уровни доверия к технической защиты информации и средствам

обеспечения безопасности информационных технологий». URL: https://check-ib.ru/docs/prikaz-fstek-rossii-76-ot-02-06-2020/ (дата обращения 13.10.2023).